HOCHSCHULE FURTWANGEN UNIVERSITY | HFU

WIRTSCHAFTSINGENIEURWESEN

Wintersemester
2018/2019

Master Thesis

Benjamin Heck
257715

Anwendung der Blockchain Technologie und Smart Contracts im Supply Chain Management

Prof. Ulrich Kallmann
Prof. Lutz Leuendorf

Abstract

Autor: Benjamin Heck

Betreuer: Prof. Ulrich Kallmann
Prof. Lutz Leuendorf

Semester: Wintersemester 2018/2019

Thema: Anwendung der Blockchain Technologie und Smart Contracts im Supply Chain Management

Inhalt: Die digitale Transformation stellt das Supply Chain Management vor große Herausforderungen. Es muss Antworten und Lösungen finden, um in einem global vernetzten Marktumfeld die Wettbewerbsfähigkeit der Supply Chain sicherzustellen. Das Konzept der Blockchain und der Smart Contracts versprechen großes Potenzial. Gerade im Bereich der Prozessautomatisierung und der Kostensenkung, durch das Entfallen bisher notwendiger Clearingstellen. Allerdings stellt sich auch immer die Frage nach der Datensicherheit und Schutz vor unbefugter Manipulation. Ziel dieser Arbeit ist es Anwendungsmöglichkeiten und Potenziale einer Blockchain und Smart Contracts im Supply Chain Management zu identifizieren und zu beschreiben

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides statt, dass ich die vorliegende Master Thesis selbstständig und ohne unzulässige fremde Hilfe angefertigt habe.

Die verwendeten Literaturquellen sind im Literaturverzeichnis vollständig zitiert.

Benjamin Heck

Brigachtal, 20 Februar 2019

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzung	Begriff
API	Application Programming Interface
BTC	Bitcoin
CPLS	Cyber-physisches Logistiksystem
CPPS	Cyber-physisches Produktionssystem
CPS	Cyber-physisches System
CPU	Central Processing Unit
DApp	Decentralized Application
DPoS	Delegated Proof of Stake
ERP	Enterprise Ressource Planning
ETH	Ether
EVM	Ethereum Virtual Machine
ICO	Initial Coin Offering
PoW	Proof of Work
PoS	Proof of Stake
PoB	Proof of Burn
PoA	Proof of Authority
PrK	Private Key
PuK	Public Key
P2P	Peer-to-Peer
SCM	Supply Chain Management
SPV	Simple Payment Verification

1. Blockchain – die nächste Revolution?

Das Internet hat die Art und Weise der Kommunikation und des Datenaustausches revolutioniert und globale Transaktionen um ein Vielfaches vereinfacht. Online-Marktplätze haben die Vertriebswege verkürzt und Social Media hat die Art und Weise, wie wir kommunizieren und wie wir Nachrichten verbreiten, grundlegend verändert. Allerdings wird für jede Transaktion eine zwischengeschaltete Clearingstelle, eine vertrauenswürdige Plattform als Vermittler benötigt. So sehr diese neuen Plattformen Menschen und Institutionen auf der ganzen Welt einander näher brachten, so sehr entstand ein neues Problem: die wachsende Marktdominanz einiger weniger Plattformbetreiber, darunter Alibaba, Ebay, Airbnb, Uber, Twitter und allen voran Google, Facebook und Amazon.

Google hatte 2017 weltweit 3.359 Mrd. registrierte Nutzer und als Suchmaschine einen Marktanteil von ca. 90%, in Deutschland sogar über 94% (Statista.com, 2018a). Durch sein Geschäftsmodell bestimmt Google, welche Suchergebnisse in welcher Reihenfolge angezeigt werden und somit was wir finden und welche Webseiten wir besuchen. Mit YouTube betreibt Google zudem eine Plattform, über die jeder, der ein Smartphone oder Kamera besitzt, eigene Inhalte hochladen und veröffentlichen kann. YouTube und Facebook verändern zunehmend, vor allem bei der nachfolgenden Generation, die Art und Weise, wie Informationen verbreitet und wahrgenommen werden. Das spielt auch für die Wirtschaft eine wichtige Rolle, da die Kanäle, potenzielle Kunden zu erreichen, diversifizieren. Facebook hat mittlerweile über 2,1 Mrd. monatlich aktive Nutzer und belegt damit Platz eins unter den sozialen Netzwerken. Auf Platz 3, 4 und 7 folgen WhatsApp (1,3 Mrd.), Facebook Messenger (1,3 Mrd.) und Instagram (0,8 Mrd.), die alle drei zu Facebook gehören (Statista.com, 2018b). Das entspricht einem Marktanteil von über 52% der monatlich aktiven Nutzer, der 10 größten sozialen Netzwerke. Egal ob aus Marketingsicht, politischen Gesichtspunkten oder Nachrichtensicht kommt man an Facebook nicht mehr vorbei. Das Unternehmen hat damit eine Position erreicht, in der es Einfluss auf die Verbreitung von Informationen nehmen kann.

Amazon ist jedem als Verkaufsplattform bekannt und Marktführer im E-Commerce. Weitaus weniger bekannt ist, dass Amazon mit Amazon Web Services auch als „Infrastructure as a service" (IaaS) und als Cloud Service Provider zunehmend an Marktanteil gewinnt. Zwar haben Google, IBM und Microsoft noch etwas Vorsprung, doch die Entwicklung der letzten Jahre deutet darauf hin, dass Amazon auch auf diesem Gebiet Marktführer werden wird. 2018 werden bereits 64% aller laufenden Applikationen (Apps) public cloud platform services über Amazon Web Services nutzen, mehr als Microsoft (45%), Google (18%) oder IBM (10%) (Statista.com, 2018c). Auch hier zeigt sich, dass der größte Teil des Datenverkehrs im Internet über Server von ein paar wenigen Unternehmen läuft.

Daten werden heute in den meisten Fällen zentral gespeichert, lokal auf den Computern und Endgeräten oder in der Cloud, und durch Remote zugänglich gemacht. Aber auch in der Cloud sind die Daten zentral auf Servern gespeichert. Die Datensicherung, die Verifizierung und Zertifizierung von Transaktionen sind bei zentraler Datenspeicherung zeit- und kostenintensiv. Dazu ist die zentrale Datenspeicherung anfällig für Angriffe von außen und für Fehlfunktionen. Die Zentralität der Datenspeicherung vereinfacht Manipulation oder Verfälschung von Informationen.

Heute werden alle Transaktionen über zentrale Plattformen abgewickelt und erfordern in der Regel einen Mittelsmann, eine Plattform, die als vertrauenswürdiger Vermittler auftritt. Sobald eine bestimmte Masse an Nutzern überschritten wird, kann eine Plattform eine marktbeherrschende Stellung einnehmen, siehe Facebook, Amazon oder Google. Durch den sogenannten Netzwerkeffekt erhöht sich der Nutzen in Abhängigkeit der Menge der Netzwerkteilnehmer. Die Plattformdominanz dieser wenigen Unternehmen bestimmt dadurch die Regeln und das Geschäftsmodell, zudem sind sie im Besitz quasi aller Daten. Amazon, Google, Facebook usw. haben also die uneingeschränkte Datenhoheit. Das bedeutet, dass die Kontrolle über die Daten an diese Plattformbetreiber übertragen werden muss. Gerade in der New Economy sind die Geschäftsmodelle auf diese Datenhoheit ausgerichtet. Facebook, Google und so weiter verdienen ihr Geld grundsätzlich auf dieser Basis.

Bereits Ende der 1990er Jahre zeigten sogenannte Peer-to-Peer (P2P) Netzwerke, wie man in einer global vernetzten Welt Datenstrukturen schaffen kann, die ohne eine Plattform als Mittelsmann auskommen. Napster machte das File-sharing populär. Nutzer konnten Musik Songs als MP3 Files direkt untereinander austauschen, was damals eine neue Bewertung des Urheberrechts notwendig machte. Letztendlich entschieden Gerichte zugunsten der Musikindustrie und Napster musste 2001 seinen Dienst einstellen. Der Fall Napster zeigte, dass P2P-Systeme das Potenzial besitzen, ganze Industrien umzugestalten, indem der Mittelsmann durch P2P-Transaktionen ersetzt wird.

Das Konzept der Blockchain baut auf der Logik der P2P-Netzwerke auf und kann das Problem der zentralen Daten-speicherung und Transaktionsvalidierung durch Dritte lösen.

1.1 Einführung Blockchain

Blockchains sind dezentrale P2P-Netzwerke, innerhalb derer Transaktionen verschlüsselt durchgeführt werden können, ohne dass eine Clearingstelle notwendig ist. Die Transaktionen werden durch das Netzwerk selbst validiert indem durch das Blockchain Protokoll Konsens geschaffen wird. Das Blockchain Protokoll bestimmt die Regeln der Validierung und fungiert gleichzeitig als transparentes Kontobuch, als sogenanntes Ledger, in dem alle Transaktionen in Blöcken gespeichert und aneinander gereiht werden. Dazu werden Transaktionen durch die Hashfunktion in ein standardisiertes Format konvertiert. Die Hashfunktion kodiert einzelne Aussagen einer Transaktion in einen Hashwert und verdichtet diese anschließend hierarchisch. Diese hierarchische Verdichtung einzelner Aussagen wird als Hashbaum oder aus Merkle Baum bezeichnet. Durch diese hierarchische Verdichtung erhält jeder Block einen individuellen Hashwert. Die Änderung einer einzelnen Aussage würde den Hashwert verändern und macht die Kodierung somit gegenüber Manipulationsversuchen sicher. Damit ein Block in die bestehende Blockchain aufgenommen wird, muss ein kryptografisches Rätsel gelöst werden. Dabei geht es darum, welche Zeichenkette einen ähnlichen Wert hat wie die Kodierung des neu aufzunehmenden Blocks. Die notwendige Anzahl an Übereinstimmungen im Hashwert wird durch das Konsensfindungs Konzept definiert und ist dadurch variierbar (Prinz and T.Schulte, 2017, p. 10). Es gibt verschiedene Konzepte der Konsensfindung wie beispielsweise Proof-of-Work oder Proof-of-Stake, auf die in Abschnitt 2.3.5 eingegangen wird. Jeder Teilnehmer des Blockchain Netzwerkes fungiert als Node (Knotenpunkt) und hat die gesamte Blockchain gespeichert. Jeder Node hat also eine identische Version des Ledgers gespeichert. Somit sind alle auf demselben Datenstand. Wenn ein Node die korrekte Zahlenfolge gefunden hat, wird der Block an die Blockchain als letzter gültiger Block angehängt. Diesen Prozess nennt man „Mining“. Da bisher kein konstruktives Verfahren für die Ableitung der zu erratenden Zeichenfolge des Hashwertes verfügbar ist, muss eine Vielzahl von Zeichenfolgen probiert werden, was entsprechende Rechenkapazität benötigt (Prinz and T.Schulte, 2017, p. 10). Je mehr Rechenkapazität ein Node also zur Verfügung stellt, desto höher ist die Wahrscheinlichkeit, dass er einen neuen Block durch Finden des korrekten Hashwertes validiert. Das erfolgreiche Mining von Blöcken wird beispielsweise in der Bitcoin Blockchain mit der Kryptowährung Bitcoin belohnt. Sobald ein Node ein Rätsel gelöst, also einen Block validiert hat, wird durch die Konsensfindung die Lösung durch das gesamte Netzwerk geprüft und übernommen. Dazu muss lediglich der Hashwert berechnet werden und der neue Block wird an die Blockchain angefügt.

Neue Transaktionen werden also zu Blöcken zusammengefasst und, nachdem sie von der Mehrheit des Netzwerks validiert wurden, der Blockchain angehängt und somit im Ledger gespeichert. Alle Teilnehmer des Netzwerkes haben jederzeit und in Echtzeit Zugriff auf die Daten der Blockchain, was nicht bedeutet, dass der Inhalt einer Transaktion für jeden sichtbar ist, da Transaktionen verschlüsselt werden. Einmal validiert und gespeichert kann eine Transaktion nicht mehr geändert werden. Eine Änderung einer Transaktion würde vom Netzwerk bemerkt werden, da sich der Hashwert ändern und so nicht mehr mit dem Wert der Blockchain übereinstimmen würde. Der Node mit der veränderten Blockchain wäre nicht mehr Teil des Netzwerkes. Theoretisch wäre es möglich eine Transaktion auf der Mehrheit der Nodes gleichzeitig zu ändern, was aber ausgeschlossen werden kann. Statistisch gesehen ist es aller-dings nicht unmöglich.

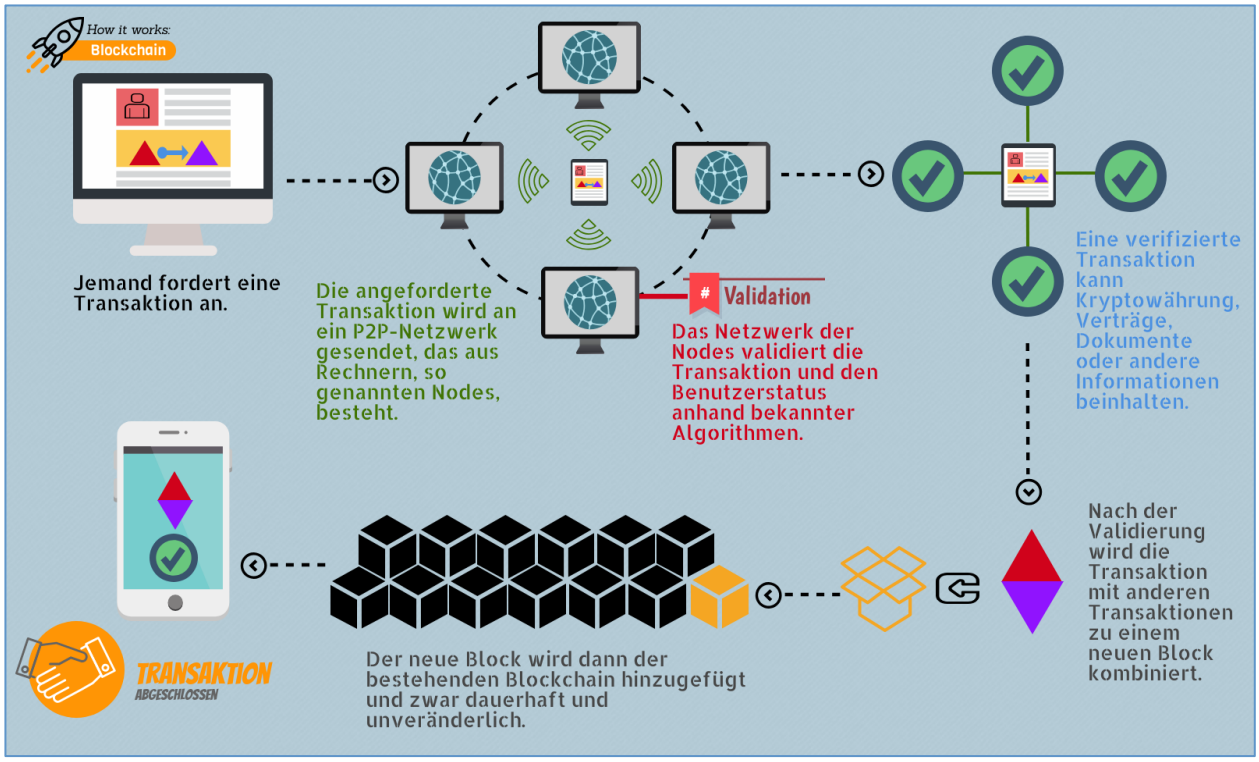

Abb. 1: Blockchain: How it works, eig. Darstellung vgl. (PWC, 2016)

Wichtigstes Merkmal ist die Dezentralität der Blockchain, wodurch zentral organisierte Informationssysteme dezentralisiert werden können. Überall wo bisher ein Vermittler in Form einer „Trusted third Party" notwendig ist, wo Transaktionen sicher verwaltet und verifiziert werden müssen, kann das Blockchain Konzept angewendet werden.

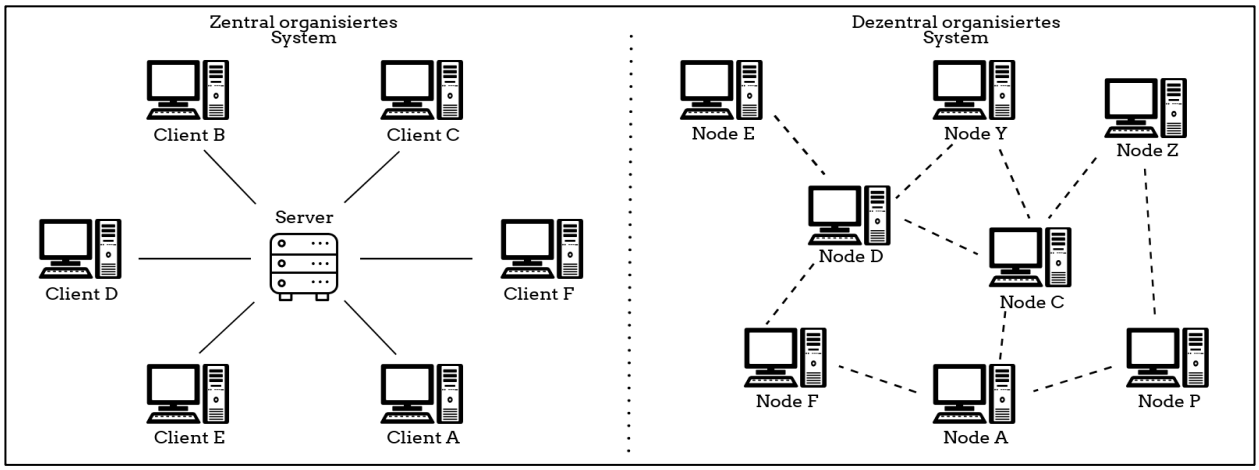

Abb. 2: Centralized vs. decentralized System, eig. Darstellung vgl. (Singhal et al., 2018)

Im Allgemeinen werden drei Gründe für die Dezentralisierung von Systemen vorgebracht (Buterin, 2017):

- **Geringe Fehleranfälligkeit** – die Ausfallwahrscheinlichkeit dezentraler Systeme ist wesentlich geringer als bei zentral organisierten Systemen, da das System auf vielen Komponenten verteilt läuft. Der Ausfall einer Komponente wird durch die anderen im Netzwerk aktiven Komponenten kompensiert. Der Ausfall eines Servers (siehe Abb. 2) kann in einem zentral organisiertem Informationssystem zum Ausfall des gesamten Systems führen. Eine Blockchain würde nur ausfallen, wenn alle Nodes gleichzeitig ausfallen.

- **Widerstandsfähigkeit gegenüber Angriffen** – durch die dezentrale Struktur des Systems fehlt es Angreifern an zentralen sensiblen Schwachstellen. Angriffe müssten auf die Mehrheit der Nodes eines Netzwerkes quasi gleichzeitig stattfinden, um nicht bemerkt zu werden.
- **Kollusionsresistenz** – es ist in dezentralen Systemen viel schwieriger für Netzwerketeilnehmer so zusammen zu arbeiten, dass sie auf Kosten anderer Teilnehmer profitieren.

Die Potenziale und Eigenschaften des Blockchains Konzeptes zusammengefasst (Prinz and T.Schulte, 2017, p. 8):

- Das Konzept der verteilten Konsensbildung kann in Geschäftsprozessen die Rolle eines vertrauenswürdigen Dritten übernehmen. Die Validierung und Zertifizierung von Transaktionen wird durch das Blockchain Protokoll und das Netzwerk übernommen. Bestehende Geschäftsmodelle vieler Institutionen und Organisationen wie beispielsweise das der Banken werden in Frage gestellt. Es ergeben sich auch neue Geschäftsmodelle, die ohne die Blockchain Technologie nicht wirtschaftlich möglich wären. Der Mittelsmann, die Trusted Third Party, wird durch das Vertrauen in das Netzwerk, besser gesagt in das Protokoll der Blockchain, ersetzt.
- In einer Blockchain können Werte abgebildet und von einem Nutzer an einen anderen transferiert werden. Die Eigentumsverhältnisse sind dabei eindeutig und transparent nachverfolgbar. Kryptowährungen sind dabei nur eine mögliche Anwendung, auch Rechte an realweltlichen, materiellen Werten wie beispielsweise Immobilien oder Grundstücken können in einer Blockchain abgebildet und gehandelt werden. Damit kann sie das Internet von einer Plattform des Kopierens und Teilens zu einer Plattform erweitern, die Herkunft und Besitz transparent protokolliert.
- Das Konzept der Smart Contracts (Kapitel 3) ermöglicht es, durch Regeln und Ausführungsanweisungen Prozesse und/oder Transaktionen auf einer Blockchain dezentral und automatisiert auszuführen. Damit eröffnet sich ein enormes Automatisierungspotenzial, was gerade unter dem Gesichtspunkt Industrie 4.0 und der Entwicklung zu cyber-physischen Systemen von großer Bedeutung ist. Gerade die Vernetzung in cyber-physischen Systemen macht eine neue, unternehmensübergreifende dezentrale Lösung zum Initiieren und Ausführen von Transaktionen notwendig, die dazu vertrauenswürdig und für jeden Netzwerkteilnehmer transparent ist.
- Alle Transaktionen in einer Blockchain sind für die Netzwerkteilnehmer sichtbar und damit nachvollziehbar. Zudem sind die Transaktionen irreversibel. Transaktionen können nicht nachträglich manipuliert oder gelöscht werden, nachdem sie in der Blockchain gespeichert wurden. Um eine Transaktion zu ändern oder zu löschen muss eine entsprechende neue Transaktion ausgeführt werden. Diese Änderungstransaktion muss wiederum vom Netzwerk validiert werden und wird dadurch für jeden sichtbar und transparent in der Blockchain protokolliert. Herkunftsnachweise und Transaktionen werden dadurch im Prinzip revisionssicher. Dies bietet ganz neue Möglichkeiten im Bereich der Compliance bis hin zur vollständig automatisierten Prüfung bisher manuell durchgeführter Prüfungen durch Wirtschaftsprüfer.

1.2 Bedeutung der Blockchain für Industrie 4.0

Der Begriff Industrie 4.0 wurde 2011 von einer Promotorengruppe der Forschungsunion Wirtschaft in Hannover vorgestellt. Die Verbände BITKOM, ZVEI und VDMA gründeten die Plattform Industrie 4.0 und veröffentlichten 2015 einen Bericht mit Umsetzungsstrategien zu Industrie 4.0. In diesem Bericht definierten sie den Begriff Industrie 4.0 wie folgt:

> *„Der Begriff Industrie 4.0 steht für die vierte industrielle Revolution, einer neuen Stufe der Organisation und Steuerung der gesamten Wertschöpfungskette über den Lebenszyklus von Produkten. Dieser Zyklus orientiert sich an den zunehmend individualisierten Kundenwünschen und erstreckt sich von der Idee, dem*

Auftrag über die Entwicklung und Fertigung, die Auslieferung eines Produkts an den Endkunden bis hin zum Recycling, einschließlich der damit verbundenen Dienstleistungen.

Basis ist die Verfügbarkeit aller relevanten Informationen in Echtzeit durch Vernetzung aller an der Wertschöpfung beteiligten Instanzen sowie die Fähigkeit, aus den Daten den zu jedem Zeitpunkt optimalen Wertschöpfungsfluss abzuleiten. Durch die Verbindung von Menschen, Objekten und Systemen entstehen dynamische, echtzeitoptimierte und selbst organisierende, unternehmensübergreifende Wertschöpfungsnetzwerke, die sich nach unterschiedlichen Kriterien wie beispielsweise Kosten, Verfügbarkeit und Ressourcenverbrauch optimieren lassen." (BITKOM et al., 2015, p. 8)

In den USA wird der Begriff „Industrial Internet" verwendet, unter dem im Prinzip dasselbe verstanden wird. General Electric und Accenture beschreiben das Industrial Internet als *„…the tight integration of the physical and digital worlds. The Industrial Internet enables companies to use sensors, software, machine-to-machine learning and other technologies to gather and analyze data from physical objects or other large data streams and then use those analyses to manage operations and in some cases to offer new, value-added services."* (Accenture and General Electric, 2014, p. 7)

Industrie 4.0 zielt darauf ab, technologische und marktwirtschaftliche Potenziale zu heben und in einem systematisierten Innovationsprozess zu erschließen. Industrie 4.0 fokussiert sich auf die digitale Durchgängigkeit des Engineerings und die vertikale Integration und Vernetzung von Produktionssystemen (Plattform I4.0, 2013, p. 24).

Ein Merkmal der Industrie 4.0, welches in Bezug zur Blockchain Technologie von wesentlicher Bedeutung ist, ist die horizontale Integration über Wertschöpfungsnetzwerke. Darunter versteht man die Vernetzung aller Prozesse und die Integration partizipierender IT-Systeme eines Netzwerkes, auch unternehmensübergreifend. Die klassische Wertschöpfungskette (Supply Chain) entwickelt sich zu einem Wertschöpfungsnetzwerk (Supply Chain Network), das aus mehreren autonom agierenden Teilnehmern besteht, wie in Abbildung 3 dargestellt. Dabei geht die Vernetzung auch über die eigentlichen Wertschöpfungsprozesse der Produktion oder der Logistik hinaus. Neben der engen Verknüpfung von Lieferanten, Unterauftragnehmern bis hin zum Kunden können auch Energielieferanten und Banken oder Zahlungsdienstleister integriert werden.

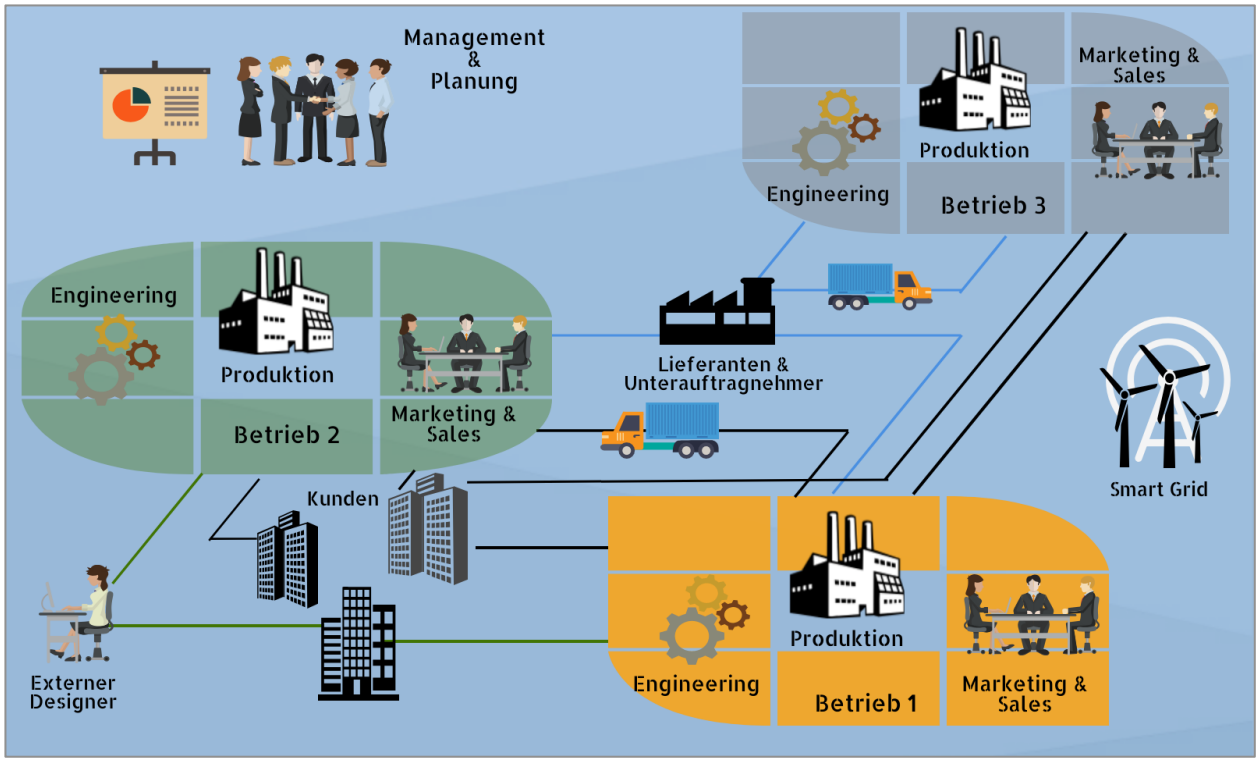

Abb. 3: Horizontale Integration, eig. Darstellung vgl. (Plattform I4.0, 2013)

Die Vernetzung zu einem Supply Chain Network wird möglich durch sogenannte cyber-physische Systeme. Ein cyber-physisches System verbindet die virtuelle mit der realen Welt. In Produktionssystemen wird von CPPS (cyber-physischen Produktionssystemen) und in der Logistik von CPLS (cyber-physischen Logistiksystemen) gesprochen. In so einem System sind Maschinen, Lagersysteme, Betriebsmittel und Transporteinheiten miteinander vernetzt und tauschen ständig Informationen untereinander aus. Lagerbestände, Lieferzeiten und alle möglichen sonstigen Informationen werden über ERP-Systeme mit Lieferanten, Unterauftragnehmern, Speditionen, Kunden, usw. ausgetauscht. Dadurch stehen Informationen zu Lagerbeständen und Bedarfen in Echtzeit zur Verfügung und die Produktion kann effizient darauf ausgerichtet werden. Durch die vollständige Vernetzung und Verfügbarkeit aller Informationen in Echtzeit ist ein cyber-physisches System in der Lage die Planung und Steuerung dezentral durchzuführen. Die dezentrale Steuerung erfordert die Kommunikation aller Komponenten in Echtzeit. Dazu müssen alle Objekte wie bspw. Maschinen, Transporteinheiten oder Lagerbereiche mit Sensoren oder entsprechenden RFID-Chips ausgestattet sein. Alle realen Objekte werden virtuell abgebildet, wodurch ein Supply Chain Network vollständig virtuell abgebildet werden kann. Durch den intensiven Datenaustausch, gerade auch organisationsübergreifend, kommt der Authentizität, Qualität und Verlässlichkeit der Daten eine entscheidende Bedeutung zu. Teilnehmer eines Supply Chain Network müssen sich auf die Echtheit und Validität der Daten verlassen können, um ausreichend Vertrauen in das Supply Chain Network aufzubauen. Cyber-physische Systeme werden Menschen, Objekte und Systeme unternehmensübergreifend miteinander vernetzen.

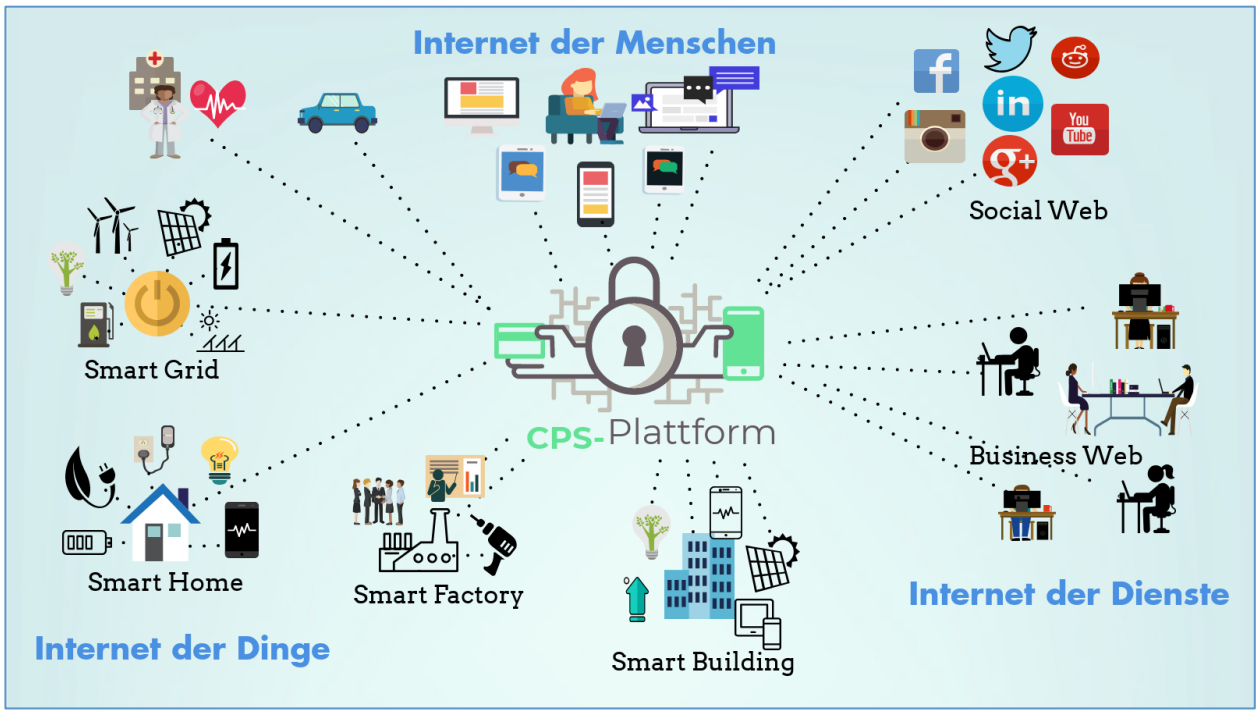

Abb. 4: Vernetzung zu cyber-physischen Systemen, eig. Darstellung vgl. (Plattform I4.0, 2013)

Die Vernetzung zu dezentralen Strukturen wird in Abbildung 4 deutlich. Vergleicht man die Struktur mit Abbildung 2 eines dezentral organisierten Systems, sieht es in dieser Abbildung zwar so aus, als ob die CPS-Plattform als zentrale Vermittlungsstelle fungiert. Sie ist aber als ein Netzwerksystem zu betrachten, welches die verschiedenen Systeme verbindet. Im Prinzip kann man den Datenaustausch innerhalb eines cyber-physischen Systems auch als Transaktionen zwischen dezentral organisierten Nodes betrachten. Jedes vernetzte Objekt eines cyber-physischen Systems kann einen Node darstellen. Hier deutet sich schon das Potenzial der Blockchain in Bezug auf Transaktionsabwicklungen in einem vernetzten System an, zudem auch durch die Fälschungssicherheit der Blockchain ein für Teilnehmer entscheidendes Kriterium erfüllt wird.

Der hohe Grad an Automatisierung und Autonomie in einem Wertschöpfungsnetzwerk betrifft die Prozesse zur dynamischen Netzwerkbildung (Verhandlung), als auch die eigentlichen Wertschöpfungsprozesse, inklusive der Planung und Steuerung. Angebot und Nachfrage sollen automatisiert zueinander finden und sich selbstständig zu effizienten, wertschöpfenden Abläufen verbinden. Produktionsaufträge und Maschinen, Transportaufträge und Logistikdienstleister sollen miteinander direkt verhandeln und dezentral gesteuert werden, um einen optimalen Wertschöpfungsprozess zu finden (BMWi, 2017, p. 10).

In der Forschungsagenda Industrie 4.0, herausgegeben vom Bundesministerium für Wirtschaft und Energie (BMWi), stellt die Arbeitsgruppe Forschung und Innovation der Plattform Industrie 4.0, Forschungsbedarf zu dem Thema Verhandlungen und Vertragsabschluss in automatisierten Wertschöpfungsnetzwerken fest. Sie stellt dabei, unteranderem, folgende Fragen (BMWi, 2017, p. 5):

- Wie können Dienstleistungsangebote hinsichtlich der angebotenen Leistung und den organisatorischen Randbedingungen spezifiziert werden, dass Computer autonom die Passfähigkeit zu den Bedarfen feststellen können?
- Wie können automatisiert Verträge zwischen Maschinen und Produkten einerseits und Produktionsaufträgen, Transportdienstleistungen, Wartungsaufträgen usw. andrerseits geschlossen werden? Wie gestalten sich Vertragsanpassungen?
- Wie können und dürfen Maschinen Verträge abschließen? Wie können Vertragsparteien automatisierter Verträge als juristische Person im Sinne des Gesetzes handeln? Wie erfolgt die Abrechnung und Bezahlung?
- Wie befähigt man Anbieter, ihre angebotenen Leistungen formal zu beschreiben und zur Verfügung zu stellen?
- Wie kann sichergestellt werden, dass Verhandlungen über die Auftragsvergabe in Echtzeit und garantiert zum vereinbarten Zeitpunkt zu einem rechtssicheren Ergebnis führen? Wie können abweichende Ziele und Rahmenbedingungen, die zur Entwurfszeit unbekannt waren, berücksichtigt werden?

Antworten auf einige dieser Fragen könnte das Konzept der Smart Contracts liefern. Smart Contracts sind Software Programme, die Bedingungen enthalten, die bei Eintreffen eines vereinbarten Ereignisses automatisch ausgeführt werden. Sehr vereinfacht dargestellt beruhen diese Programme auf dem IF→THEN→ELSE Prinzip. So könnte beispielsweise ein Logistikdienstleister automatisch beauftragt werden, wenn Produkte zur Auslieferung im Fertigteillager eingehen. Die Blockchain fungiert dabei als Plattform zur Ausführung sogenannter dezentraler Apps (DApps). Auf das Konzept der Smart Contracts wird in Kapitel 3 ausführlich eingegangen.

1.3 Supply Chain Management 4.0

Dem Supply Chain Management (SCM) kommt in global vernetzten Wertschöpfungsnetzwerken eine zentrale Bedeutung zu. Um erfolgreich am Markt zu agieren, ist es für Unternehmen entscheidend, Wertschöpfungsketten und die zunehmende Vernetzung zu Wertschöpfungsnetzwerken effektiv, effizient und dabei flexibel zu gestalten. Unternehmen sind dabei zunehmend gefordert, kurzfristig auf Nachfrageschwankungen und auf die immer kürzer werdenden Produktlebenszyklen zu reagieren.

Aufgabe des SCM ist es, leistungsfähige Supply Chains zu entwickeln, zu steuern und diese zu Supply Chain Networks zu vernetzen. Göpfert konkretisiert SCM als *„…moderne Konzeption für Unternehmensnetzwerke zur Erschließung unternehmensübergreifender Erfolgspotenziale mittels der Entwicklung, Gestaltung, Lenkung und Realisation effektiver und effizienter Güter-, Informations-, Geld- und Finanzflüsse.*" (Göpfert, 2013, p. 32)

Im Rahmen der digitalen Transformation zu Industrie 4.0, und damit zu SCM 4.0, geht es vor allem darum, starre Supply Chains zu dynamischen Supply Chain Networks zu entwickeln (Abb.5).

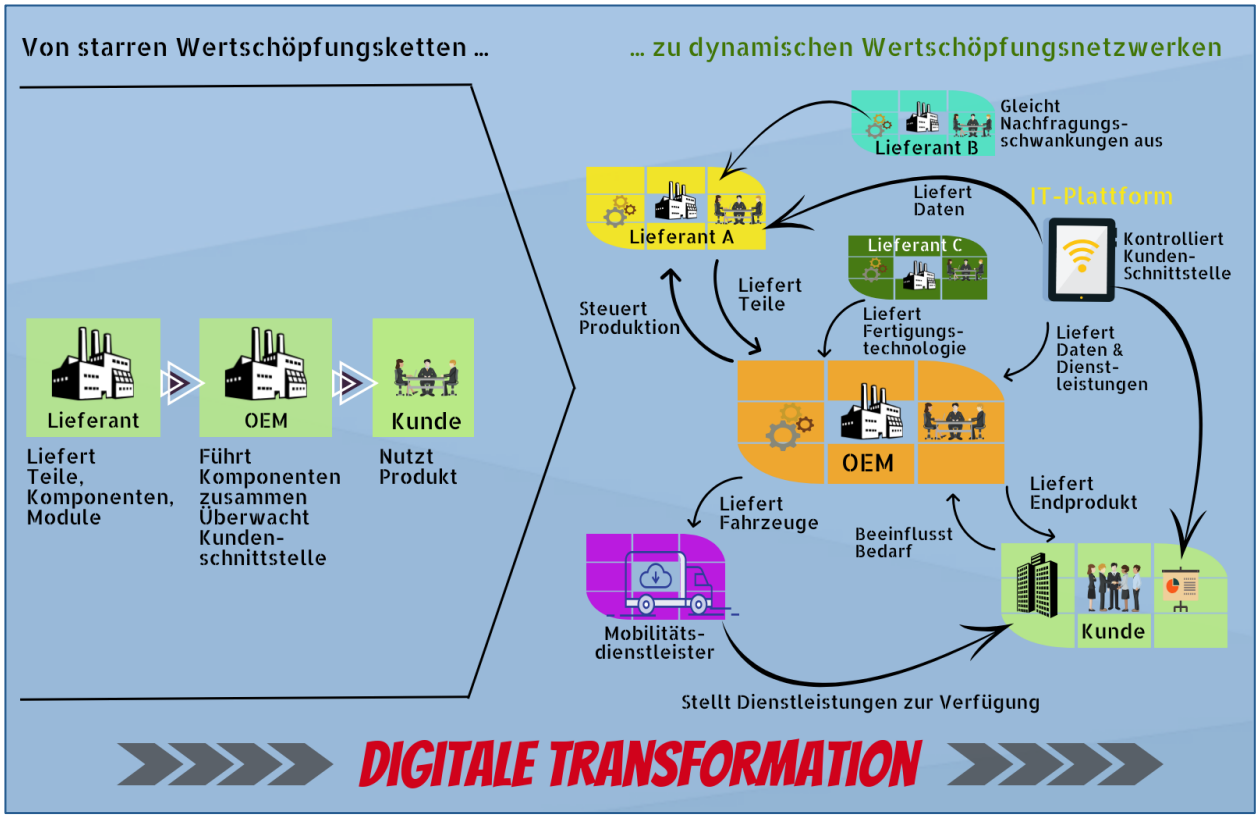

Abb. 5: Transformation der Supply Chain, eig. Darstellung vgl. (Zillmann and Appel, 2016)

Die Logistik ist zentraler Bestandteil der horizontalen Integration in Supply Chain Networks. Die Logistik innerhalb des Netzwerkes umfasst dabei die gesamte Supply Chain, vom Rohstofflieferanten über die Produktion bis hin zum Endverbraucher. Die bereits erwähnte Arbeitsgruppe Forschung und Innovation der Plattform I4.0 erwartet einen disruptiven Wandel der Logistik:

> *„Grundsatzfragen der Algorithmik und der Anwendung im Zusammenwirken autonomer Logistikeinheiten müssen beantwortet werden. Ferner gilt es, die Dynamikanforderungen der flexiblen und kleinteiligen Produktion logistisch bedienen zu können, beispielsweise durch die automatische Kontrahierung freier Kapazitäten und durch die Automatisierung der Disposition."* (BMWi, 2017, p. 6)

Die intelligente Vernetzung von Produktion und Logistik zu cyber-physischen Systemen erzeugt enorme Mengen an Daten. Diese Datenströme effizient zu verarbeiten und daraus effektive Strategien abzuleiten ist Aufgabe des SCM 4.0. Planung und Steuerung eines cyber-physischen Systems, erfolgen autonom und dezentral auf Grundlage lokaler Informationen. Dazu müssen „Missionen" implementiert werden, die durch das SCM zu definieren sind. Darüber hinaus kommt dem Ressourcenmanagement mehr und mehr Bedeutung zu. Darunter versteht man die Vernetzung von Energie, Daten und Materialflüssen zu komplexen Ökosystemen, die die digitale Transformation zu Industrie 4.0 mit sich bringt. In der wettbewerbsorientierten Marktwirtschaft trägt effektives Management des Working-Capital[1] und

[1] Working Capital = Umlaufvermögen – kurzfristige Verbindlichkeiten

eine optimierte cash-to-cash cycle time[2] entscheidend zum Unternehmenserfolg bei, wobei auch hier das SCM maßgeblich am Erreichen der Ziele gefordert ist.

Damit Unternehmen Vertrauen in ein Supply Chain Network aufbauen, muss sichergestellt werden, dass Transaktionen zuverlässig und fälschungssicher abgewickelt werden können. Weiterhin müssen die Daten transparent und dauerhaft gespeichert werden und nachverfolgbar sein. Beide Kriterien erfüllt das Blockchain Konzept.

1.4 Aufgabenstellung, Zielsetzung und Methode

Die digitale Transformation stellt das SCM also vor große Herausforderungen. Es muss Antworten und Lösungen finden, um in einem global vernetzten Marktumfeld die Wettbewerbsfähigkeit der Supply Chain sicherzustellen. Das Konzept der Blockchain und der Smart Contracts versprechen großes Potenzial. Gerade im Bereich der Prozessautomatisierung und der Kostensenkung durch das Entfallen bisher notwendiger Clearingstellen. Allerdings stellt sich auch immer die Frage nach der Datensicherheit und Schutz vor unbefugter Manipulation.

Ziel dieser Arbeit ist es Anwendungsmöglichkeiten und Potenziale einer Blockchain und Smart Contracts im Supply Chain Management zu identifizieren und zu beschreiben. Dabei soll auch auf mögliche Schwachstellen und Risiken eingegangen werden. Im ersten Schritt wird die Geschichte und das Konzept der Blockchain vorgestellt. Anhand verfügbarer Literatur und verschiedener White Paper der bekanntesten Blockchain Konzepte, soll die Funktion der Blockchain verständlich und kompakt beschrieben werden. Anschließend wird das Konzept der Smart Contracts erklärt und anhand eines ersten Anwendungsbeispiels das Potenzial der Prozessoptimierung angedeutet. Im vierten Kapitel sollen an einem konkreten Beispiel Anwendungsmöglichkeiten in einer Supply Chain identifiziert werden. Dazu wird ein Szenario entwickelt welches möglichst realistisch Potenziale, Risiken und Schwachstellen herausabreitet. Eine Prozesskostenrechnung und eine Wirtschaftlichkeitsbetrachtung sollen abschließend den wirtschaftlichen Nutzen belegen.

[2] Cash-to-cash cycle time = Ø Lagerdauer + Ø Inkassoperiode + Ø Lieferantenzahlungsziel

2. Blockchain

Heutzutage wird die Blockchain immer noch vorrangig mit Bitcoin in Verbindung gebracht. Kryptowährungen erlebten seit Anfang 2017 einen regelrechten Hype. Der Wert für ein Bitcoin erreichte im Dezember 2017 kurzzeitig seinen vorläufigen Höchststand von knapp 20.000 US$ / Bitcoin. Einschätzungen von Finanzanalysten über die künftige Entwicklung des Bitcoin Kurses bis 2030 reichen von 0 bis 1.000.000 US$ / Bitcoin. Auch andere Kryptowährungen erlebten einen rasanten Kursanstieg, zudem werden immer mehr Kryptowährungen am Markt gehandelt. Bis heute gibt es allerdings kaum Möglichkeiten, mit Kryptowährungen zu bezahlen, und so kann über die zukünftige Wertentwicklung nur spekuliert werden. Blockchain als Technologie um Netzwerke zu schaffen, innerhalb derer Transaktionen auf Basis von Vertrauen, Transparenz und Fälschungssicherheit der Daten durchgeführt werden können, wird dagegen die Entwicklung zu Industrie 4.0 maßgeblich beeinflussen.

2.1 Geschichte der Blockchain

Bereits in den 1990ern Jahren wurden erste Konzepte zur kryptografisch abgesicherten Verkettung einzelner Blöcke beschrieben und 1998 auch ein Mechanismus für eine dezentralisierte digitale Währung durch Nick Szabo.[3] Im Jahr 2000 wurde durch Stefan Konst eine allgemeine Theorie zur kryptografisch abgesicherten Verkettung erarbeitet *„...bei der Ecken eines beliebigen Graphen, entsprechend den zwischen ihnen existierenden Kanten, mittels kryptographischer Verfahren miteinander verkettet werden.*"(Konst, 2000, p. 60) Daraus leitete Konst ein Schema ab, mit dessen Hilfe die Authentizität und Reihenfolge einer Log-Datei überprüft werden kann und das Fehlen von Einträgen erkannt wird (Konst, 2000, p. 60). In diesem Ansatz ist das Konzept eines dezentral verteilten Datenbanksystem noch nicht enthalten.

Nachdem im Oktober 2008, zum Höhepunkt, der unteranderem durch die Lehman Brothers Pleite ausgelösten Finanzkrise, die amerikanische Regierung 700 Milliarden Dollar zur Rettung der Banken bereitgestellt hatte, veröffentlichte eine Person oder Gruppe unter dem Pseudonym Satoshi Nakamoto im November 2008 ein White Paper mit dem Title „Bitcoin: A Peer-to-Peer Electronic Cash System". Darin wird ein System zum Durchführen von elektronischen Transaktionen beschrieben, das ohne einen Mittelsmann auskommt und dennoch absolut vertrauenswürdig ist (Nakamoto, 2008). Nakamoto wird als Erfinder des Bitcoins und als Ersteller des Genesis-Blockes in die Geschichte eingehen. Er beschreibt ein elektronisches Zahlungssystem, das vollständig auf einer dezentralen Struktur aufbaut und ohne eine vertrauenswürdige Vermittlerstelle auskommt. Dadurch ist es möglich Währungseinheiten direkt von Computer zu Computer zu transferieren ohne Banken oder andere Institutionen. Nach einem ersten Ansatz durch Nick Szabo kann das Bitcoin Konzept als Geburtsstunde der digitalen Währung betrachtet werden (Rosenberger, 2018, p. 1), manche sprechen sogar von der Geburt einer Revolution.

Es wird spekuliert, dass dieses Papier als Reaktion auf die Finanzkrise veröffentlicht wurde, da die Banken offensichtlich ihre Position als vertrauenswürdige Zwischeninstanz bei Finanztransaktionen missbraucht und die Finanzkrise durch maßlose Spekulationen ausgelöst hatten. Ob sich allerdings hinter Satoshi Nakamoto eine Person oder eine Gruppe verbirgt, ist bis heute ungeklärt. Man findet keinerlei Spuren von Nakamoto im Internet, seit 2011 ist er oder sie gar nicht mehr aktiv. Zuvor hatten mehrere Personen Kontakt über Email mit Nakamoto, allerdings wurden die Mails stets über anonyme Hosting-Services und durch einen kryptischen Schlüssel gesichert versendet (Rosenberger, 2018, p. 26).

[3] Nick Szabo ist Informatiker, Rechtswissenschaftler und Kryptograph, bekannt für seine Forschung zu digitalen Verträgen und digitaler Währung. Er schloss sein Studium an der University of Washington 1989 mit einem Abschluss in Informatik ab. Er hat eine Honorarprofessur an der Universidad Francisco Marroquín inne ("Nick Szabo," 2018).

Interessanterweise kommt der Begriff Blockchain in keinem der bisher vorgestellten Konzepte vor. Sowohl im Konzept von Konst der kryptographischen Verkettung sowie in Nakamoto´s Bitcoin White Paper wird zwar von Blöcken gesprochen, der Begriff Blockchain kommt allerdings an keiner Stelle vor. Programmierer übertrugen das Bitcoin Konzept in einen Code und erschufen damit das Protokoll hinter der Kryptowährung Bitcoin. Dieses Protokoll wurde Blockchain genannt. Das Protokoll war von Anfang an open source und wurde in der Folge oft kopiert und modifiziert. Es konnte also jeder Kryptowährungen erschaffen, wodurch heute viele Kryptowährungen gehandelt werden wie z.B. Dash, Monero, Litecoin uvm. Das Bitcoin Protokoll ist einzig darauf ausgelegt, Transaktionen durchzuführen, die Werte von einem Node zu einem anderen transferieren. Vitalik Buterin erkannte das Potenzial der Blockchain als dezentral verteiltes Rechennetzwerk.

2013 veröffentlichte er das White Paper zu Ethereum. Genau wie Bitcoin ist Ethereum ein dezentrales Blockchain Netzwerk. Anstatt lediglich als Transaktionsplattform zu agieren stellt Ethereum das technische Fundament zur Verfügung, um Smart Contracts und Programmcodes, sogenannte Decentralized Applications, DApps auszuführen (Rosenberger, 2018, p. 54). Der innovative Ansatz besteht in dem Einfügen eines Abstraction Layers[4], sodass Transaktionen aus verschiedenen Anwendungen auf den Programmcode verallgemeinert werden können, der auf allen Ethereum-Nodes laufen kann (Singhal et al., 2018, p. 221). In 2014 konnte Ethereum durch eine Crowdfunding Kampagne 18 Millionen USD innerhalb von 6 Wochen einsammeln. Seit Juni 2015 steht die Ethereum Blockchain jedem als Plattform zur Entwicklung von möglichen Anwendungen zur Verfügung. Neben mehreren Clients stehen auch verschiedene Programmiersprachen zur Verfügung, mit denen man Smart Contracts programmieren kann. Inzwischen konnte sich Ethereum als eine Art Standard für die Anwendungsentwicklung auf der Blockchain etablieren. Die Enterprise Ethereum Alliance, bestehend aus vielen namhaften Unternehmen, Startups und Forschungsgruppen, unterstützt Ethereum dabei, die Blockchain Technologie weiterzuentwickeln (Rosenberger, 2018, p. 60). Auch bei Ethereum gibt es eine Kryptowährung, genannt Ether, die auf der Ethereum Blockchain als Zahlungsmittel verwendet werden kann. Für Transaktionen werden bei Ethereum Gebühren erhoben, die in Ether abgerechnet werden.

Quasi als Antwort auf Ethereum wurde in China eine Blockchain, inkl. einer Kryptowährung namens NEO entwickelt, die bereits quantencomputertauglich aufgesetzt sein soll. Während Ethereum auf eine eigen entwickelte Skriptsprache setzt, wurde NEO über Standard-Programmiersprachen entwickelt, sodass jeder, der etwas vom Programmieren versteht, in der Lage ist, auf der Plattform zu arbeiten, ohne sich vorab spezielle Kenntnisse aneignen zu müssen. Smart Contracts können dadurch leichter und somit von einer größeren Anzahl Nutzern aufgesetzt werden. NEO möchte traditionelle Vermögenswerte digital abbilden und mittels digitaler Zertifikate in der Blockchain hinterlegen. Auf die gleiche Weise sollen Identitäten wie Handelsregistereinträge oder Grundbucheinträge rechts- und fälschungssicher dezentral in der Blockchain hinterlegt werden. Der Gründer Da Hongfei möchte NEO als anerkannte Institution in China etablieren (Rosenberger, 2018, p. 55).

Die bisherige Entwicklung der Blockchain Anwendungen wird in drei Phasen unterteilt. Blockchain 1.0 umfasst die Kryptowährungen, Blockchain 2.0 Smart Contracts und Blockchain 3.0 die Weiterentwicklung zu dezentralen autonomen Organisationseinheiten (Prinz and T.Schulte, 2017, p. 8). Die Idee einer dezentralen Organisation nimmt das Konzept der traditionellen Organisationen und dezentralisiert es. Anstelle einer hierarchischen Struktur, die von einer Gruppe von Menschen verwaltet wird, die persönlich interagieren und Eigentum über das Rechtssystem kontrollieren, beinhaltet eine dezentrale Organisation eine Gruppe von Personen, die gemäß einem im Code festgelegten Protokoll miteinander interagieren (Voshmgir and Kalinov, 2017).

[4] Eine Hardwareabstraktionsschicht ist eine Schicht eines Betriebssystems, die den Kernel und alle übrige Software von der Hardware isoliert ("Hardwareabstraktionsschicht," 2015).

2.1.1 Kryptowährungen

Kryptowährungen sind digitale Währungen mit einem meist dezentralen, stets verteilten und kryptografisch abgesicherten Zahlungssystem. Sie ermöglichen einen bargeldlosen Zahlungsverkehr ohne Abhängigkeit von Banken oder Behörden. Die Blockchain ist das System, auf dem Transaktionen erfasst, beschrieben und dauerhaft gespeichert werden (Prof. Dr. Bendel, 2018). Man spricht in diesem Zusammenhang auch von sogenannten Tokens. In der Bitcoin Blockchain spricht man beispielsweise von Bitcoins. Über das Blockchain Protokoll werden Regelsätze definiert, die auf kryptographischen wirtschaftlichen Anreizmechanismen basieren, die festlegen, unter welchen Umständen Transaktionen validiert und neue Blöcke erstellt werden. Im Fall der Bitcoin Blockchain werden Nodes, die einen neuen Block erstellen, für das Bereitstellen der notwendigen Rechenleistung mit Bitcoins entlohnt.

Neben der Funktion als Kryptowährung sind Tokens auch auf andere Art verwendbar. Es wird unterschieden in vier Arten von Tokens:

- **Usage Token** werden benötigt um einen Service zu nutzen. Token Besitzer haben keine Rechte innerhalb des Netzwerkes, sondern der Besitz berechtigt lediglich zum Nutzen eines Services, im Fall von Bitcoin zum Nutzen der Blockchain als Zahlungssystem (Voshmgir and Kalinov, 2017, p. 22).
- **Utility Token** haben eine bestimmte Funktionalität innerhalb der Blockchain für Produkte und/oder Dienstleistungen (Hahn and Wons, 2018, p. 10).
- **Asset-backed Token** sind an ein Anlagegut oder Aktivposten gebunden und stellen einen Anspruch auf den entsprechenden Wert (z.B. Gold, Immobilien oder Rohstoffe) dar (Hahn and Wons, 2018, p. 11).
- **Equity Token** sind vergleichbar mit Unternehmensanteilen in Form von Aktien oder einer Unternehmensbeteiligung. Diese Token werden zur Unternehmensfinanzierung verwendet mit dem Versprechen einer Gewinnbeteiligung und/oder Mitspracherecht innerhalb des Unternehmens (Hahn and Wons, 2018, p. 10).

2.1.1.1 BITCOIN - BTC

Bitcoin ist die bekannteste Kryptowährung, dennoch gibt es bis heute kaum Möglichkeiten, Produkte oder Dienstleistungen mit Bitcoins zu bezahlen. Bitcoins dienen hauptsächlich als Spekulationsobjekt an speziellen Bitcoin Börsen wie z.B. bitcoin.de oder Binance. Die Preisfindung ist dabei allerdings bisher völlig unklar. Anders als bei Aktien, deren Wert durch eine Unternehmensbewertung wenigstens einigermaßen nachvollziehbar ist, haben Bitcoins keinen Gegenwert den man bestimmen kann. Man kann eine Parallele zu Gold feststellen. Der Goldpreis wird an den Börsen durch Angebot und Nachfrage ermittelt. Als Einflussfaktoren gelten dabei der US Dollar Kurs, Zinssätze, der Ölpreis sowie Preise anderer Rohstoffe. Zudem spielen andere Einflussfaktoren wie die allgemeine Wirtschaftslage und politische Ereignisse eine Rolle. Einzig die Preisuntergrenze kann bei Bitcoin definiert werden. Wie beim Gold entstehen Kosten für das Betreiben einer Mine. Beim Abbau von Gold sind das u.a. Kosten für Lohn und Betriebsmittel, beim Minen von Bitcoins entstehen die Kosten hauptsächlich durch den hohen Strombedarf, neben der benötigten Hardware (Rosenberger, 2018, p. 21). Der Strombedarf ist mittlerweile so hoch, dass die Kosten für Strom in vielen Ländern den Wert der erzeugten Bitcoins übersteigen. So belaufen sich die Kosten für Strom, um ein Bitcoin zu minen, in Deutschland auf 14.275 US$ (Jeff, 2018). Bei einem Bitcoin Wert von ca. 5.700 US$ (Stand September 2018) wird schnell klar, dass sich das Minen nicht mehr rechnet. Dementsprechend werden Bitcoins sowie die meisten anderen Kryptowährungen in Ländern mit niedrigen Stromkosten erzeugt.

Um die Werthaltigkeit einer Währung zu gewährleisten ist eine Begrenzung notwendig. Bei herkömmlichen Währungen übernehmen diese Aufgabe die Zentralbanken. Um die Werthaltigkeit einer virtuellen Währung zu gewährleisten muss eine künstliche Verknappung im Protokoll verankert werden. Im Bitcoin Protokoll wurde die Erzeugung von Bitcoins in den ersten 4 Jahren auf 50 Bitcoins alle 10 Minuten beschränkt. Alle 4 Jahre halbiert sich diese Menge sodass 2012 nur noch 25 Bitcoins und entsprechend seit 2016 nur noch 12,5 Bitcoins pro Block erzeugt werden. Bis dieser Wert rechnerisch auf null gesunken ist werden 21 Millionen Bitcoins generiert sein, danach werden keine weiteren mehr erzeugt (Rosenberger, 2018, p. 87).

2.1.1.2 ETHER – ETH

Die auf Ethereum Blockchain verwendete Kryptowährung wird Ether genannt. Genau wie Bitcoins kann Ether als bargeldloses Zahlungsmittel verwendet werden. Die Ethereum Blockchain wurde entwickelt, um als Plattform zum Ausführen von DApps zu agieren. Ether kann von Anwendungsentwicklern genutzt werden, um Transaktionsgebühren zu erheben und angebotene Dienste in Rechnung zu stellen. Anders als bei Bitcoin ist die maximale Anzahl an Ether nicht begrenzt. Derzeit werden jedes Jahr ca. 18 Millionen Ether erzeugt, um so eine künstliche Nachfrage zu erzeugen (Rosenberger, 2018, p. 54). Während bei Bitcoin das Minen von neuen Blöcken mit einem festen Wert an Bitcoins (z.Z. 12,5 BTC) belohnt wird, erhält man bei Ethereum, neben einer gewissen Anzahl an Ether, zusätzlich sogenanntes Gas. Die Menge an Gas orientiert sich an der Komplexität der in dem Block enthaltenen Transaktionen. Der Kurs von Gas orientiert sich an der tatsächlich benötigten Rechenleistung und dem daraus resultierenden Strom- und Hardwarebedarf (Rosenberger, 2018, p. 54). Wie Bitcoin und viele andere Kryptowährungen hat Ether seit Anfang 2017 einen rasanten Kursverlauf erlebt und kurzfristig die 1.000€ Marke durchbrochen.

2.1.2 Marktentwicklung

Wie bereits erwähnt erreichte der Hype um Kryptowährungen im Dezember 2017 seinen vorläufigen Höhepunkt. Der Preis für ein Bitcoin erreichte knapp die 20.000 US$ Marke, ein Ether war im Januar 2018 kurzzeitig über 1.100 US$ wert (Abb.6+7). Dem rasanten Wachstum folgte ein regelrechter Absturz. Ob der Abwärtstrend sich fortsetzt oder lediglich ein Zwischentief darstellt ist vollkommen unklar. Expertenschätzungen reichen vom totalen Verfall des Bitcoin Kurses auf null US$ bis hin zu einem Wert von einer Million US$ für einen Bitcoin in den kommenden Jahren.

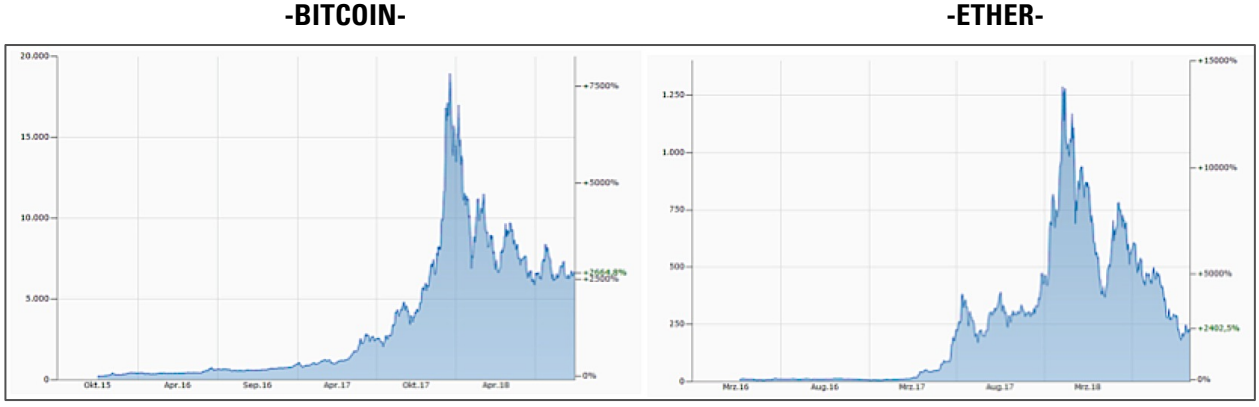

Abb. 6: Marktentwicklung 2015-2018 Bitcoin & Ether, Quelle Finanzen.net (Stand Oktober 2018)

Bitcoin ist mit 120,6 Mrd. US$ Marktkapitalisierung die am meisten gehandelte digitale Währung. Ether und alle anderen Kryptowährungen werden in den meisten Fällen durch den Tausch mit Bitcoins erworben.

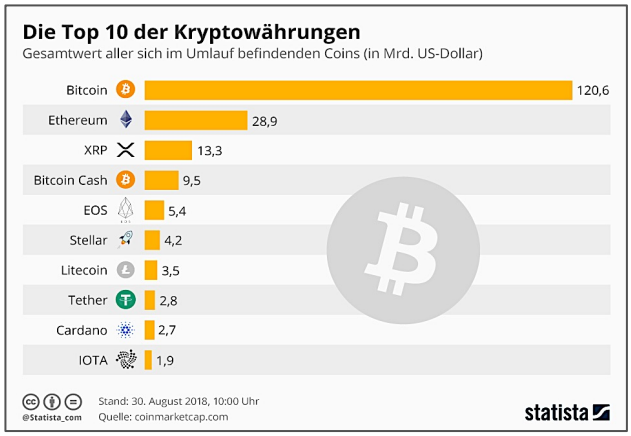

Abb. 7: Marktkapitalisierung Kryptowährung, Quelle (Nier, 2018)

Bitcoins können an speziellen Börsen gegen herkömmliche Währung getauscht werden. Zudem wird bei vielen Initial Coin Offerings, kurz ICO, über Bitcoin Transaktionen Kapital eingesammelt. Im Gegenzug werden Token ausgegeben, die selbst wiederum als Kryptowährung gelten können. 2017 wurden so rund 5,4 Mrd. US$ investiert und in den ersten sieben Monaten 2018 bereits über 14 Mrd. US$ (https://de.statista.com/infografik/11517/volumen-von-ico-finanzierungsrunden-pro-monat/).

2.2 Warum Blockchain?

In dem Whitepaper zu Bitcoin geht Nakamoto auf das Problem ein, dass bei Zahlungstransaktionen vertrauenswürdige Institutionen, in der Regel Banken, notwendig sind. Zahlungen im Internet und in der globalen Wirtschaft werden heute in so gut wie allen Fällen über Finanzinstitute abgewickelt. Das bedeutet, eine Bank überweist eine bestimmte Menge an Währung vom Konto des Senders auf das Konto des Empfängers. Sender und Empfänger vertrauen darauf, dass die Bank die Transaktion entsprechend den vereinbarten Bedingungen durchführt und nicht verändert oder rückgängig macht. Dieser Service verursacht natürlich Kosten, die durch Sender und Empfänger getragen werden müssen, in Form von Transaktionsgebühren, Kontoführungsgebühren etc. Diese Kosten könnten durch Barzahlungen umgangen werden, wobei auch das Vertrauensproblem gelöst wäre. Direkte Zahlungen sind ohne eine dritte Partei nicht möglich, außer durch persönlichen Kontakt und der Verwendung von Bargeld. Nakamoto schlägt ein elektronisches Zahlungssystem vor, das auf kryptografischen Nachweis anstelle von Vertrauen basiert und es zwei bereitwilligen Parteien möglich macht, Transaktionen direkt, ohne einen Mittelsmann, auszuführen. Das System macht es rechnerisch unmöglich, Transaktionen zu widerrufen oder nachträglich zu ändern, was beide Parteien vor Betrug schützt. Zudem könnten standardisierte Treuhandmechanismen implementiert werden. Ein dezentral organisiertes P2P-Netzwerk liefert durch Verwendung eines Zeitstempels den rechnerischen Nachweis der chronologischen Reihenfolge durchgeführter Transaktionen (Nakamoto, 2008).

Nakamoto geht also speziell auf den Anwendungsfall um Finanztransaktionen durchzuführen ein. Das Konzept kann allerdings auch auf andere Bereiche ausgelegt werden, bei denen Werte den Besitzer wechseln sollen. Beispielsweise können Eigentumsrechte bei Immobilienverkäufen über dieses System übertragen werden. Das würde den Notar als vertrauenswürdige dritte Instanz überflüssig machen, und die Notargebühren würden entfallen. Grundbucheinträge können transparent, nachweis- und unverfälschbar in der Blockchain gespeichert werden. Gleiches könnte für Rechtstitel oder Unternehmensregister gelten. Der Prozess der Eigentumsübertragung kann deutlich beschleunigt werden. Überall da, wo die Integrität von Dokumenten auf Echtheit und Richtigkeit nachweisbar sein soll, kann das Blockchain Konzept angewendet werden. Bisher müssen Daten und Dokumente mithilfe einer digitalen Signatur versehen werden, um Vertrauenswürdigkeit zu erreichen. Digitale Signaturen sind aufwendig und erfordern ebenso eine dritte vertrauenswürdige Instanz, deren Service bei Inanspruchnahme entlohnt werden muss. Weitere Beispiele sind Diplome, Zertifikate oder Abschlussurkunden von Hochschulen oder anderen Ausbildungseinrichtungen, Zulassungsstellen für PKW und die damit einhergehende Verwaltung, Elektronische Patientenverwaltung bei Krankenhäusern und –kassen sowie niedergelassenen Ärzten, Registrierung und Verwaltung von Patenten usw. (Welzel, 2017). Auch über die Möglichkeit, den Blockchain Ansatz für Wahlen einzusetzen, wird schon debattiert. Die wesentliche Eigenschaft der Blockchain ist die Transparenz aller durchgeführten Transaktionen. Sie kann dadurch Vertrauen in Systeme bilden, da die Echtheit und Herkunft der Daten jederzeit validiert werden kann. Öffentliche Einrichtungen und die Politik sehen sich immer mehr der Anforderung ausgesetzt, ihr Handeln öffentlich zu rechtfertigen und zu dokumentieren. Dazu werden Ausgaben, die durch Steuermittel oder andere öffentliche Mittel finanziert werden, kritisch hinterfragt und eine transparente Buchführung gefordert. In diesem Zusammenhang könnten auch öffentliche Haushalte, oder Ein- und Ausgaben von Parteien, Verbänden oder Hilfsorganisationen transparent dokumentiert werden. Bürokratie könnte abgebaut und möglicher Korruption und Manipulationsversuchen effektiv vorgebeugt werden.

Vor allem für das Supply Chain Management interessant ist die Möglichkeit, über den Blockchain Ansatz Herkunftsnachweise eindeutig und nicht manipulierbar zu erstellen. Vorstellbar ist, die gesamte Produkthistorie über alle Baugruppen abzubilden, angefangen von Rohstoffchargen über einzelne Bauteile von Zulieferern, zu Baugruppen und ausgelieferten Fertigprodukten, die bereits beim Kunden im Einsatz sind. Ein gutes Beispiel ist die Luftfahrtindustrie, in der eine intensive Dokumentenpflicht herrscht und Flugzeuge 20 Jahre und länger im Einsatz sind. Produktions- und Wertschöpfungsketten sowie Wartungsintervalle könnten über die gesamte Lebensdauer einfach und sicher nachverfolgbar dokumentiert werden. Gleiches gilt für medizinische Produkte oder Lebensmittelwaren und Eigentumsnachweise beim Handel mit besonders wertvollen Gütern wie beispielsweise Antiquitäten oder Kunstobjekten (Welzel et al., 2017).

2.2.1 Trust and Integrity

In Zeiten von Fake News und immer neuen Datenskandalen sinkt das Vertrauen der Bevölkerung in Politik, Medien und Wirtschaft. Das Edelman Trust Barometer zeichnet eine Welt des Misstrauens öffentlichen Einrichtungen, Nachrichten und Unternehmen gegenüber (Abb.8). So überwiegt 2018 nur noch in fünf Ländern das Vertrauen in die Institutionen.

Abb. 8: A World of Distrust, Quelle (Ries et al., 2017)

Immer neue Datenskandale wie der Diebstahl von über 50 Millionen Facebook Nutzerdaten Anfang 2018 oder die durch Edward Snowden ausgelöste NSA Affäre lassen auch das Vertrauen in Internet Plattformen seit Jahren sinken. Gerade in den USA hat der Index des Vertrauensbarometers seit 2017 einen dramatischen Sprung von elf Punkten nach unten gemacht. Angeheizt von der Fake News Kampagne des amerikanischen Präsidenten trauen immer weniger Menschen Nachrichten und Social Media Plattformen (Abb.9).

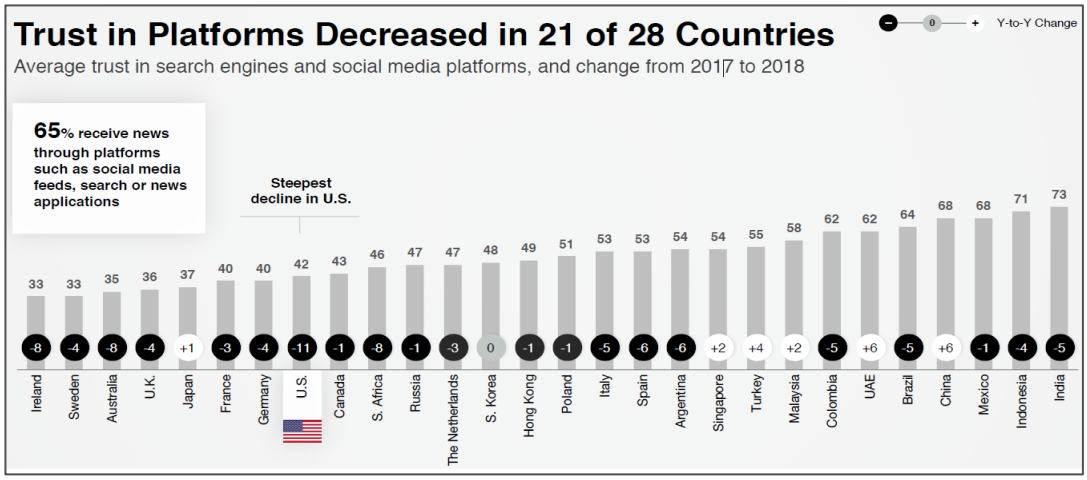

Abb. 9: Trust in Plattforms, Quelle (Ries et al., 2017)

Für Unternehmen ist Vertrauen in Geschäftspartner umso wichtiger, je enger es in Wertschöpfungsnetzwerken mit anderen Unternehmen vernetzt ist. Dabei profitieren Kunden, Zulieferer, Partner und Banken im gleichen Maße von der Konnektivität innerhalb eines Wertschöpfungsnetzwerkes. Wertschöpfung entsteht durch den Fluss von Waren und Dienstleistungen über das Wertschöpfungsnetzwerk hinweg. Dabei werden ständig Werte und Eigentumsrechte von einem Partner auf den anderen übertragen. Vermögenswerte können dabei materieller oder immaterieller Natur sein. Immaterielle Werte können finanzieller Art sein wie bspw. Anleihen, intellektueller Art wie bspw. Patente, oder digital wie bspw. Musik. In jedem Fall wird der Transfer von Werten in Unternehmen immer durch die Buchführung dokumentiert und muss bei Prüfungen durch entsprechende Nachweise belegbar sein. Dabei ist jeder Teilnehmer eines Wertschöpfungsnetzwerkes für die korrekte Buchführung verantwortlich. Das bedeutet: in heutigen Wertschöpfungsnetzwerken hat jeder Partner eine eigene Buchführung und muss darauf vertrauen, dass seine Partner ebenfalls eine korrekte Buchführung betreiben und dabei die gleichen Daten und Informationen aufzeichnen (Abb.10). Dieses System ist ineffektiv, mit hohen Kosten verbunden und fehleranfällig.

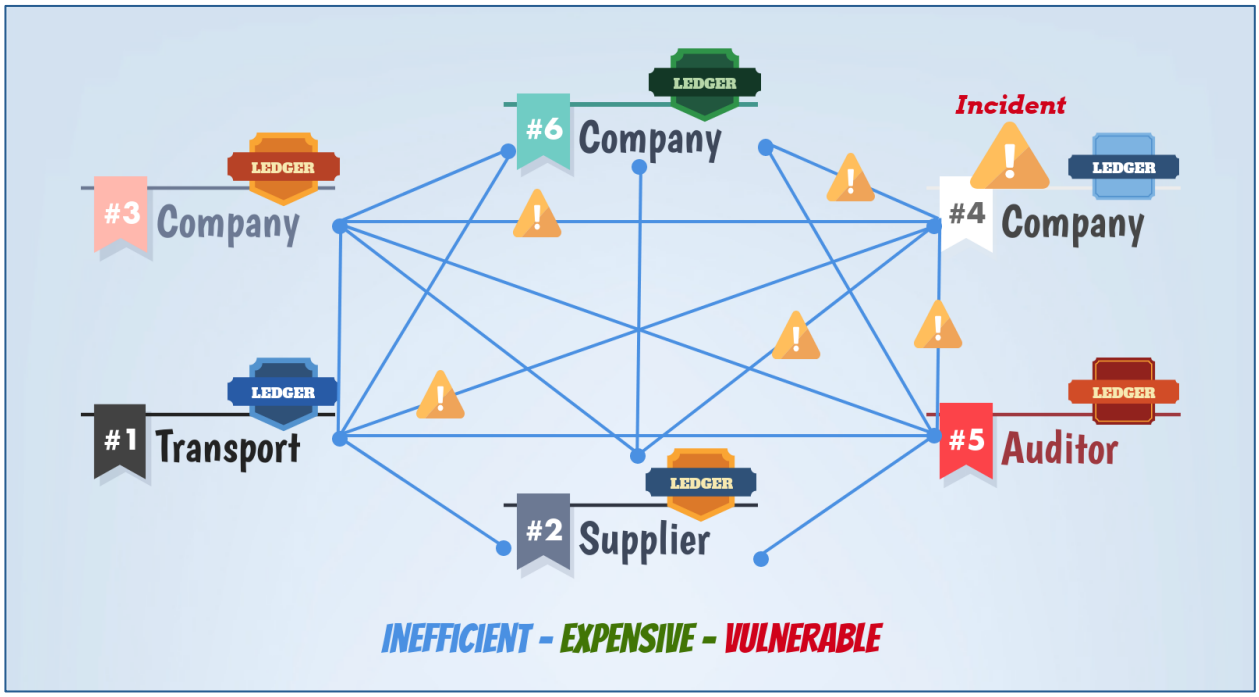

Abb. 10: The Trust Problem, eig. Darstellung vgl. (Cole and Gorman, 2017)

Die Lösung ist eine Buchführung, über ein geteiltes Ledger (Hauptbuch) (Abb.11). Alle Transaktionen werden dezentral in diesem Ledger dokumentiert und sind für jeden Teilnehmer nachvollziehbar. Das Blockchain Konzept mit seiner dezentraler P2P-Architektur kann den Ansatz eines geteilten Ledgers abbilden. Dabei fungiert jeder Teilnehmer als Node des Netzwerkes und ist dementsprechend an der Konsensbildung beteiligt und im Besitz des aktuellen Datenstandes. Durch die Fälschungssicherheit, der Unveränderlichkeit und der Konsensbildung in einer Blockchain kann Vertrauen über alle Teilnehmer eines Wertschöpfungsnetzwerkes gebildet werden. Zudem können Prozesse vereinfacht und vermittelnde Stellen abgebaut werden. Dadurch können Lieferzeiten und Kosten gesenkt werden. Da die Blockchain als fälschungssicher gilt, ist sie theoretisch auch sehr einfach auditierbar und könnte teure Audits durch Wirtschaftsprüfungsgesellschaften überflüssig machen oder den Aufwand solch einer Prüfung drastisch reduzieren. Herkunftsnachweise können eindeutig und für jeden nachvollziehbar jederzeit einsehbar sein. Dabei wird jedoch sichergestellt, dass jeder Teilnehmer nur die Transaktionen einsehen kann, an denen er beteiligt ist oder eine Berechtigung erteilt wurde. Es ist davon auszugehen, dass an Wertschöpfungsnetzwerken nur Partner teilnehmen, die in irgendeiner Form an dem Netzwerk partizipieren. Ein Netzwerk, das für jeden frei zugänglich ist, wie bspw. die Bitcoin Blockchain, wird von Unternehmen in der Regel nicht erwünscht sein.

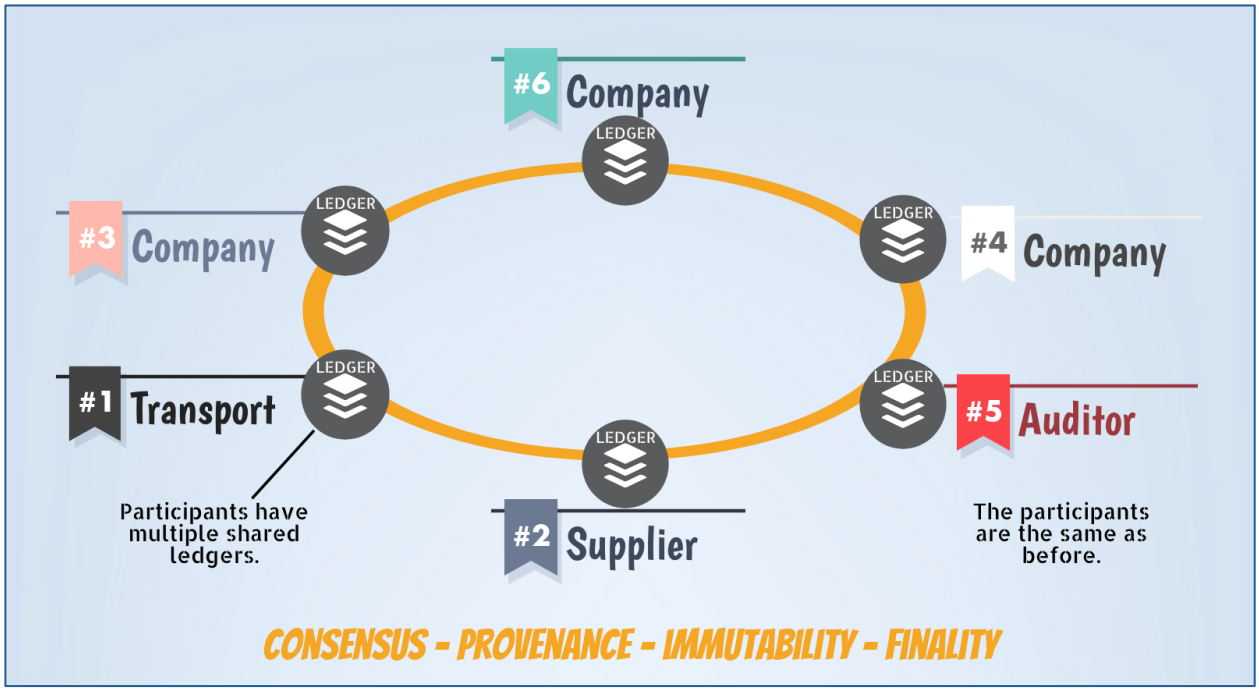

Abb. 11: The Solution to the Trust Problem, eig. Darstellung vgl. (Cole and Gorman, 2017)

2.2.2 Decentralization

Heute werden alle Transaktionen von zentral organisierten Plattformen abgewickelt und erfordern in der Regel eine vertrauenswürdige dritte Partei. Banken oder Unternehmen wie Amazon, Google oder eBay haben die Datenhoheit. Das bedeutet, dass die Kontrolle über die Daten an diese Institutionen übertragen werden muss, um eine Transaktion durchzuführen. Gerade in der New Economy sind die Geschäftsmodelle dieser Unternehmen auf die Datenhoheit ausgerichtet. Facebook, Google und so weiter verdienen ihr Geld grundsätzlich auf dieser Basis.

In seinem Buch „The Business Blockchain" beschrieb William Mougayar die Möglichkeiten der Dezentralisation von Geschäftsprozessen:

> Decentralization „…*will include banking without banks,..., e-commerce without eBay, registrations without government officials overseeing them, computer storage without Dropbox, transportation services without Uber, computing without Amazon Web Services, online identities without Google,... Take any services and add "without previous center-based authority," and replace it with "peer-to-peer, trust-based network," and you will start to imagine the possibilities.*" (Mougayar and Buterin, 2016)

Des Weiteren beschreibt er die charakteristischen Eigenschaften von dezentral basierten Services (Mougayar and Buterin, 2016):

- Schnelle und direkte Abrechnung
- Keine zwischen geschalteten Verzögerungen
- Umfassende Identifikation und Reputation
- Flache Struktur ohne Overhead
- Vertrauenswürdiges Netzwerk
- Widerstandsfähigkeit gegen Angriffe
- Keine Zensur
- Keine zentrale Fehlerstelle

- Governance-Entscheidungen im Konsens
- Peer-to-Peer-Kommunikation

Zusammenfassend kann die Blockchain durch drei Definitionen beschrieben und definiert werden (Mougayar and Buterin, 2016):

- **Technisch** gesehen ist die Blockchain eine Datenbank, die ein dezentral verteiltes Ledger verwaltet, das transparent und durch jeden Netzwerkteilnehmer geprüft werden kann.
- Aus **Unternehmenssicht** betrachtet ist die Blockchain ein Netzwerk für das Durchführen von Transaktionen. Und eine Plattform auf der Vermögenswerte, Waren und Rechte zwischen Partnern, ohne die Notwendigkeit von Vermittlern, transferiert werden können.
- **Rechtlich** gesehen validiert die Blockchain Transaktionen und ersetzt, zuvor notwendige Clearing Stellen.

2.3 Blockchain – How it works

Die grundlegende Funktionsweise der Blockchain wurde bereits in Kapitel 1 beschrieben. Um im weiteren Schritt Anwendungsmöglichkeiten im Supply Chain Management zu identifizieren und zu erarbeiten, ist es zuvor notwendig, ein grundlegendes Verständnis der Blockchain Technologie zu erlangen.

Die Bitcoin Blockchain ist darauf ausgelegt, die Kryptowährung Bitcoin zu handeln. Die zur Zeit wohl am weitesten entwickelte Blockchain Ethereum, verfolgt den Ansatz, als Plattform zum Betreiben von Applikationen zu dienen. Unternehmen wie IBM, Microsoft oder SAP haben sich zu Konsortien zusammengeschlossen, um Anwendungsmöglichkeiten für die Wirtschaft zu entwickeln. Vor allem Smart Contracts versprechen ein breites Anwendungsfeld im Supply Chain Management.

2.3.1 Grundprinzip der Blockchain

In der Blockchain werden Transaktionen zu Blöcken zusammengefasst und in einem dezentral verteiltem Ledger fortgeschrieben. Jeder Block generiert aus den enthaltenen Daten der Transaktionen durch den sogenannten Merkle Baum einen Hashwert, der in Kombination mit dem Hashwert des vorangegangen Blocks einen neuen Hashwert generiert (Abb.12). Der Hashwert des letzten Blockes wird also aus allen bis dahin enthaltenen Transaktionen generiert.

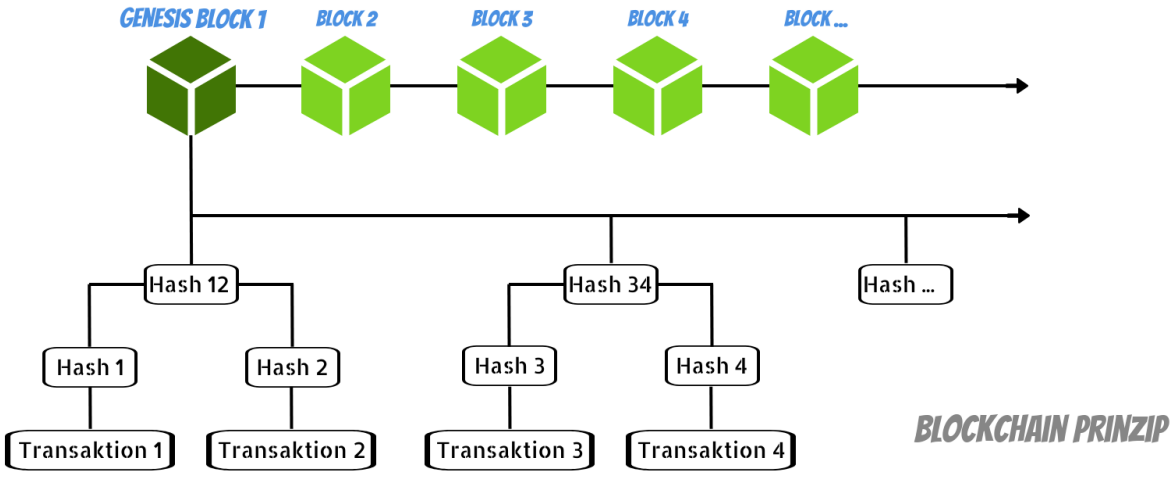

Abb. 12: Blockchain Prinzip, eig. Darstellung vgl. (Rosenberger, 2018, p. 18)

Der Hashwert ist Teil des sogenannten Headers. Ein Block besteht aus dem Header, der Blockgröße in Bytes, der Transaktionsliste und aus dem Transaktionszähler. Der Header wiederum enthält neben dem Hashwert des vorangegangenen Blocks und der Versionsnummer des Blockchain Protokolls einen Zeitstempel (Timestamp), den Schwierigkeitsgrad (Difficult Target) der verwendeten Konsensbildungs Regeln (bspw. Proof of Work), den Hashwert (Merkle Root), generiert durch den Merkle Baum aus den enthaltenen Transaktionen und einen Wert, der zufällig beim Mining Prozess entstanden ist (Nonce) (siehe Abbildung 13).

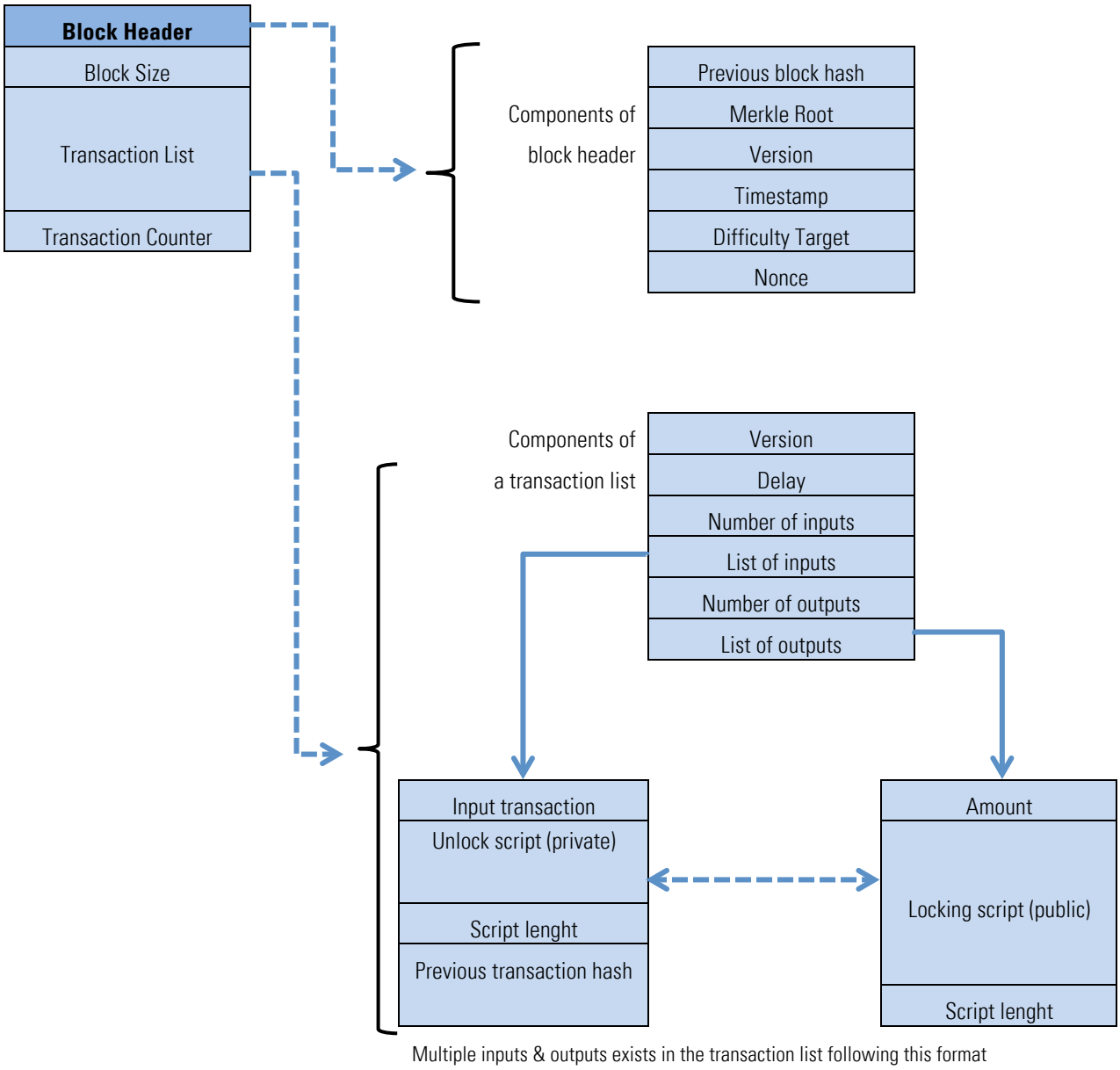

Abb. 13: Vereinfachte Blockstruktur, eig. Darstellung vgl. (Dhillon et al., 2017, p. 17)

Der Merkle Root, generiert durch den Merkle Baum, macht jeden Block einzigartig und ist dadurch einwandfrei identifizierbar. Das Prinzip des Merkle Baums ist in Abbildung 14 dargestellt. In diesem Beispiel bilden acht Transaktionen (Tx1...Tx8) die Basis zur Generierung des Merkle Roots, aus dem der Block spezifische Hashwert hervorgeht.

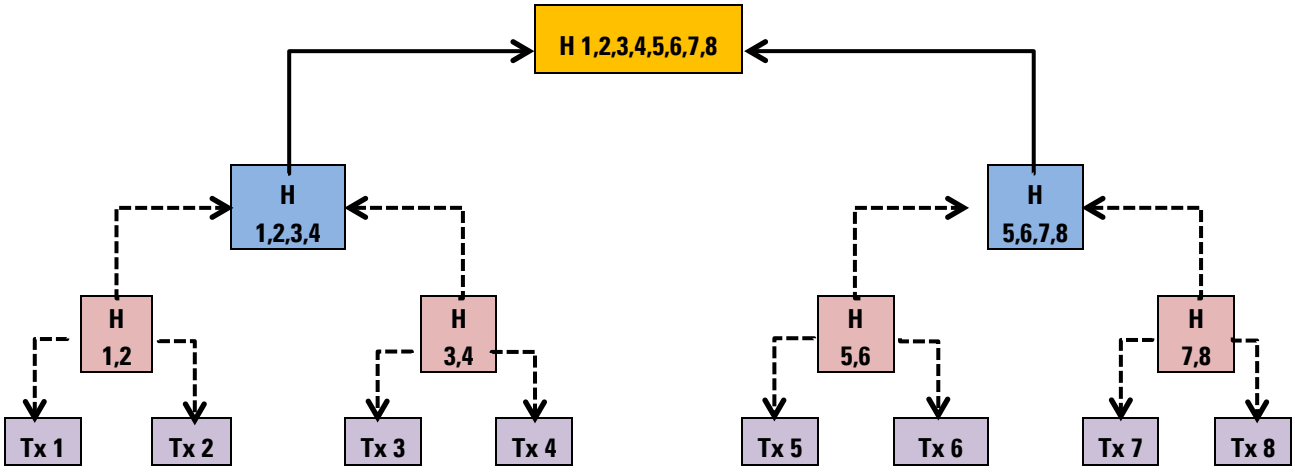

Abb. 14: Merkle Baum, eig. Darstellung vgl. (Dhillon et al., 2017, p. 22)

Die Daten jeder Transaktion werden durch die Hash Funktion SHA-256[5] verschlüsselt. Die Hash Funktion wandelt die Informationen der Transaktionen in einen Hashwert. Und die Kombination der Hashwerte generiert einen neuen Hashwert, bis man auf der obersten Ebene den Merkle Root erhält, der den Hashwert aller enthaltenen Transaktionen repräsentiert. SHA-256 gehört zu der SHA-2 Familie, die noch andere Varianten wie bspw. SHA-512 enthält, und wird in der Bitcoin Blockchain verwendet. Die Ethereum Blockchain verwendet KECCAK-256 als kryptografisches Verfahren, welches der SHA-3 Familie zugeordnet wird und eine Weiterentwicklung der SHA-2 Familie ist.

Nehmen wir an, die Transaktion Tx1 enthält folgende Information:

Unternehmen A liefert an Unternehmen B die Menge X zum Zeitpunkt Y

Der Hashwert zu Tx1 lautet[6]:

8A738C63F772D7EC53655D0FCB041F30B376632644F57151C5151B86E1C690DD

Die Information in Tx2 lautet:

Spedition X übernimmt den Transport von Standort A zu B

Der Hashwert zu Tx2 lautet:

CF34414EE540167498EFE4A24078B6F7FEA7646C0A8D0CA5D8EA20573785DDDD

Um den Hashwert Tx1,2 zu erhalten werden die Werte Tx1 und Tx2 mit derselben Funktion verschlüsselt.

Der Hashwert Tx1,2 lautet:

EB4DE97676C4E552BE2160B86E24BBD835FF44D309F9E2111E3193988A769C94

So werden der Hashwert der Transaktionen Tx1-8 zu einem Block zusammengefasst und der Hashwert aus allen enthaltenen Werten Tx1,2,3,4,5,6,7,8 ermittelt → Merkle Root. Zusammen mit dem Hashwert des vorangegangenen Blocks, dem Difficult Target, des Timestamps und einem beim Minen des Blocks zufällig generiertem Wert, Nonce genannt, entsteht so der neue Hashwert des Blocks, der den aktuellen Stand der gesamten Blockchain repräsentiert.

[5] SHA-256 – Ein von der NSA entwickeltes kryptografisches Verfahren.

[6] Hashwert generiert mit https://passwordsgenerator.net/sha256-hash-generator/

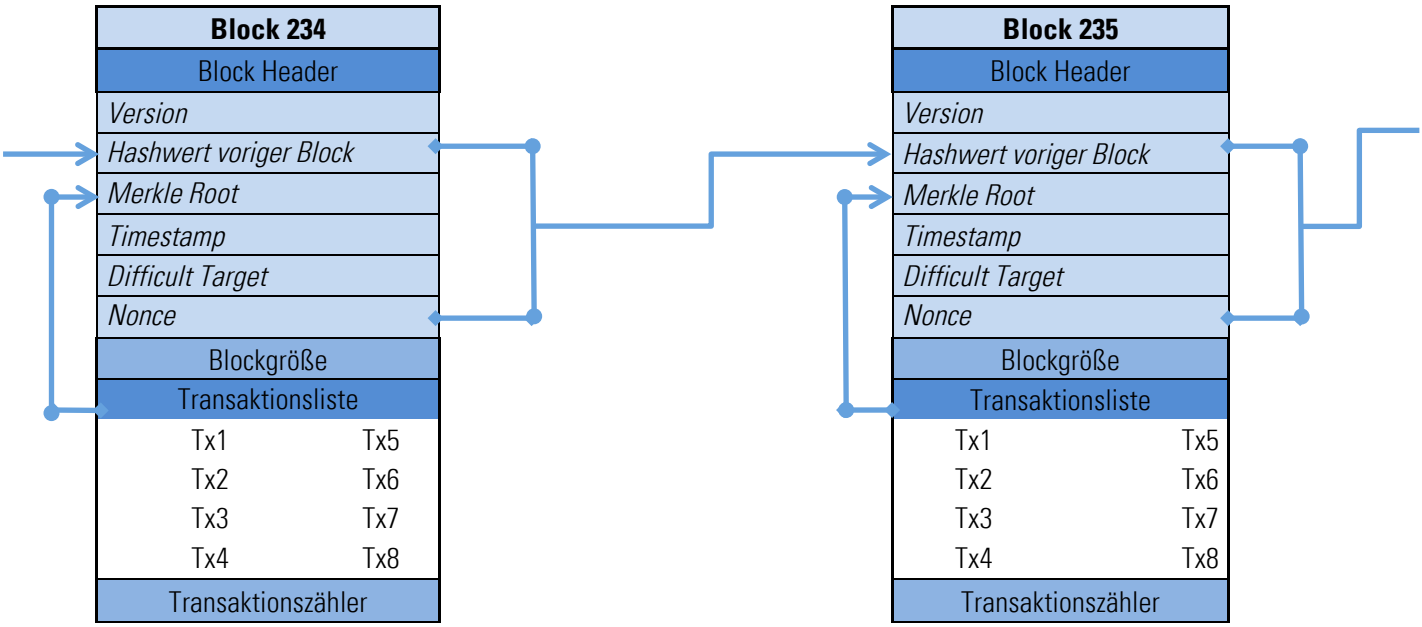

Abb. 15: Struktur eines Blockes, eig. Darstellung

Der Block Header muss folgende Bedingungen erfüllen (Drescher, 2017, p. 140):

1. Er muss den gültigen Hashwert des vorangegangen Blocks enthalten.
2. Er muss einen validierten Merkle Root enthalten, erzeugt durch den Merkle Baum aus den enthaltenen Transaktionen.
3. Er muss den korrekten Difficult Target enthalten.
4. Sein Zeitstempel muss nach dem Timestamp des vorangegangen Blocks datiert sein.
5. Er muss einen Nonce enthalten.
6. Der Hashwert generiert aus diesen Werten (Hashwert voriger Block, Merkle Root, Difficult Target, Timestamp und Nonce) erfüllt die Bedingung Hashwert < Difficult Target.

2.3.2 Mining

Den Prozess, einen neuen Block aus mehreren Transaktionen zu erstellen und der Blockchain anzuhängen, nennt man Mining (deutsch: schürfen). Der Begriff ist aus dem Bergbau abgeleitet, da es wie beim Goldschürfen darum geht etwas zu finden. Im Fall der Blockchain bedeutet das die Lösung für ein mathematisches Rätsel als erster zu finden.

Neu erzeugte Transaktionen werden durch die dezentrale Struktur des Netzwerkes über jeden verbundenen Node verteilt und damit veröffentlicht. Die Transaktion ist allerdings noch unbestätigt, also wurde noch nicht ausgeführt. Bevor eine unbestätigte Transaktion an einen anderen Node weitergeleitet wird, verifiziert jeder Node die Gültigkeit der Transaktion. Dazu prüft der Node anhand einer langen Checkliste[7] ob die im Blockchain Core Protokoll festgelegten Bedingungen erfüllt werden (Antonopoulos, 2017, p. 220). Der erste Node, der eine ungültige Transaktion findet sortiert diese aus. So wird sichergestellt, dass nur gültige Transaktionen im Netzwerk veröffentlicht werden. Gültige Transaktionen, die neu im Blockchain Netzwerk zur Validierung veröffentlicht wurden, werden zunächst in einem Transaktionspool gesammelt, bis ein Miner sie in einen neuen Block aufnimmt. Ein Miner kann jeder beliebiger Node des Netzwerkes sein, dazu ist eine spezielle Software auf dem Node zu installieren, die den Mining-Prozess ausführen kann. Nachdem ein Miner einen neuen Block erstellt hat, benötigt dieser einen Header, bevor er von der

[7] Die Checkliste variiert je nach Blockchain Protokoll. In der Anlage ist beispielh. die Checkliste des Bitcoin Protokolls aufgeführt.

Blockchain akzeptiert werden kann. Dieser Block wird Candidate Block genannt. Der Header des Candidate Blocks hat bereits den Merkle Root generiert, der durch den Merkle Baum aus den enthaltenen Transaktionen der Transaktionsliste berechnet wird. Der Header enthält bereits auch den Hashwert des letzten Blocks der Blockchain, der wie bereits beschrieben den gültigen Hashwert aller bis dahin in der Blockchain validierten Transaktionen repräsentiert. Der Header ist also bis auf den Nonce bereits vollständig. Der Nonce ist ein 32-Bit-Wert. Aufgabe des Miners ist es, den richtigen Nonce zu finden. Dazu muss er einen Nonce raten und mit ihm den Hashwert des Candidate Blocks berechnen. Der dadurch erzeugte Hashwert wird mit dem Difficult Target verglichen. Ist der Wert höher, ist die Bedingung nicht erfüllt und der Miner muss einen anderen Nonce ausprobieren. Dieser Prozess wird Proof of Work genannt und erfordert eine hohe Rechenleistung, da eine sehr große Menge an Werten ausprobiert werden muss, bis der richtige Nonce gefunden wird. Es gibt keine andere Möglichkeit, den Nonce zu erhalten oder gar zu berechnen. Das Difficult Target wird durch das Blockchain Protokoll festgelegt. In der Bitcoin Blockchain ändert sich dieser Wert alle zwei Wochen nach 2.016 Blocks. Findet ein Miner nun den richtigen Nonce, wird die Bedingung erfüllt.

Als Beispiel dient wieder die SHA-256 Funktion (Singhal et al., 2018, p. 189):

Schwierigkeitsziel: 00000000000000**79BC**0000000000000000000000000000000000000000000000

Hashwert: 00000000000000**79BB**3655D0FCB041F30B376632644F57151C5151B86E1C690DD

Beide Werte haben die gleiche Anzahl Nullen zu Beginn (14) und der Wert 79BB ist niedriger als 79BC, somit ist die Bedingung erfüllt. Je mehr Nullen das Schwierigkeitsziel hat, desto schwerer ist die Lösung zu finden. Durch das Setzen von einer unterschiedlichen Anzahl Nullen wird die durchschnittliche Zeit zum Finden der Lösung auf zehn Minuten geregelt (Singhal et al., 2018, p. 190).

Der Miner, der einen neuen validen Block findet, veröffentlicht ihn umgehend im gesamten Netzwerk. Jeder Node validiert, ob der Miner das Rätsel korrekt gelöst hat, indem einfach der Nonce mit dem Difficult Target verglichen wird, und prüft, ob der Wert geringer ist. Dann werden die Transaktionen des neuen Headers anhand des Merkle Baums validiert. Wenn alle Transaktionen validiert werden konnten, wird der Block der auf dem Node lokal gespeicherten Blockchain angehängt und so über das ganze Netzwerk verteilt (Singhal et al., 2018, p. 191).

In einem Blockchain Netzwerk gibt es natürlich mehrere Miner, die um die Validierung eines Blocks konkurrieren. Je mehr Miner aktiv sind, desto höher wird der Schwierigkeitsgrad gesetzt, dementsprechend wird mehr Rechenleistung zum Lösen des Rätsels benötigt. Als Anreiz, dem Netzwerk Rechenleistung zur Verfügung zu stellen, erhält derjenige, der als erster den korrekten Nonce eines Candidate Blocks findet, eine definierte Menge an Bitcoins als Belohnung., zur Zeit 12,5 BTC pro Block. Zusätzlich erhält der Miner eines Blocks noch Transaktionsgebühren, die der Sender einer Transaktion abgeben muss. Jeder neue Block enthält eine sogenannte Coinbase Transaktion, die beim erfolgreichen Minen des Blocks 12,5 BTC erzeugt und dem Miner überweist (Dhillon et al., 2017, p. 11). Wie bereits erwähnt werden so neue Bitcoins erzeugt, die Belohnung halbiert sich alle 210.000 Blocks, ca. alle vier Jahre, bis der Wert rechnerisch Null erreicht, was bei 21 Millionen Bitcoins der Fall sein wird.

Anhand der Abbildung 16 wird der Mining Prozess nochmals schrittweise beschrieben (Singhal et al., 2018, p. 190):

1. Ein Miner nimmt Transaktionen aus dem Transaktionspool in einen neuen Block auf. Im Fall der Bitcoin Blockchain so viele Transaktionen bis zu einer Menge von 1 MB. Dieser Block wird Candidate Block genannt. Aus den neu aufgenommenen Transaktionen wird mittels des Merkle Baums der ***Merkle Root*** generiert.
2. Der Header des Candidate Block übernimmt den Hashwert des aktuellsten Blocks der Blockchain (***Hashwert voriger Block***). Bis auf den ***Nonce*** sind nun alle Daten des Header enthalten.
3. Der Miner sucht nun den richtigen Nonce. Dazu wird der zu probierende Nonce mit dem Hashwert des vorigen Blocks, des Merkle Roots, des Timestamps und dem Difficult Traget gehasht. Der dadurch generierte Wert wird mit dem Difficult Target verglichen und geprüft, ob die Bedingung Hashwert < Difficult Target erfüllt wird. Der Miner ändert solange den Nonce Wert, bis die Bedingung erfüllt wird.
4. Wenn ein Miner den korrekten Nonce gefunden hat, veröffentlicht er umgehend den Block dem Netzwerk. Jeder Node der den Block erhält, prüft nochmals ob die Bedingung Hashwert < Difficult Target erfüllt ist.

Dazu muss nur der Header des neuen Blocks geprüft werden. Dann werden die enthalten Transaktionen anhand des Merkle Roots geprüft. Wenn alle Transaktionen validiert werden konnten, wird der Block der lokal gespeicherten Blockchain angefügt und so über das Netzwerk verbreitet (Singhal et al., 2018, p. 191).

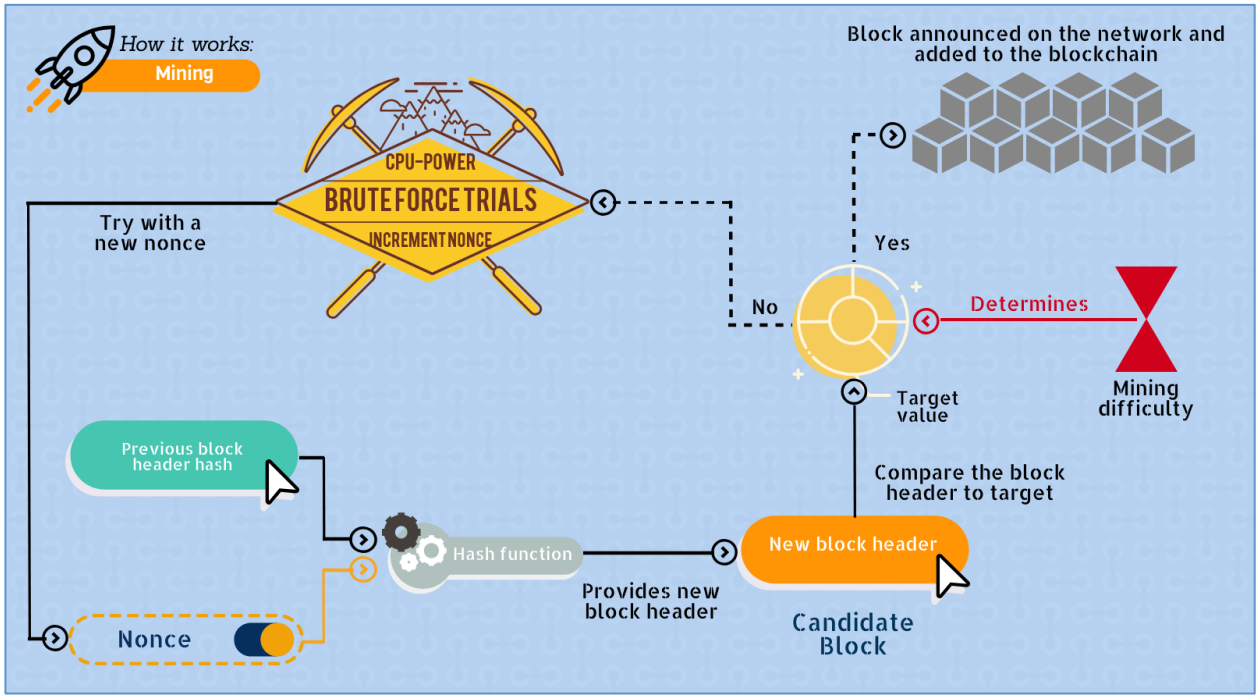

Abb. 16: Mining Prozess, eig. Darstellung vgl. (Dhillon et al., 2017, p. 11)

Fullnode vs. Simple Payment Verification (SPV)

Jeder Node hat also die gesamte Blockchain lokal gespeichert. Je länger eine Blockchain aktiv ist, desto mehr Blöcke enthält sie und entsprechend steigt der Speicherbedarf. Die Bitcoin Blockchain hat bspw. mittlerweile eine Größe von ca. 185 GB erreicht (Statista.com, 2018d). Nodes, die die gesamte Blockchain lokal gespeichert haben, werden als Fullnode bezeichnet. Sie sind die wesentlichste Komponente einer Blockchain, da sie als dezentrales P2P-Netzwerk die Grundlage bilden. Fullnodes bauen und pflegen ihre eigene Kopie der Blockchain lokal. Sie sind bei der Transaktionsvalidierung nicht auf das Netzwerk angewiesen, da sie autark sind. Sie sind nur daran interessiert, neu veröffentlichte Blöcke zu kennen, die von anderen Nodes vorgeschlagen werden, sodass sie ihre lokale Kopie nach der Validierung eines Blocks aktualisieren können (Singhal et al., 2018, p. 209)

Bei einer Größe von 185 GB, wie bei der Bitcoin Blockchain, wird es für manche Nodes unattraktiv, so viel Speicherplatz vorhalten zu müssen, um am Netzwerk partizipieren zu können. Beispielsweise haben Notebooks und normale Working Stations in Relation gesehen wenig Speicherplatz zur Verfügung. Um Transaktionen validieren zu können ist es nicht notwendig, eine Kopie der gesamten Blockchain gespeichert zu haben. Die Bitcoin Blockchain hält dazu ein Konzept vor, das sich Simple Payment Verification (SPV) nennt.

Bei diesem Konzept wird anstelle der gesamten Blockchain lediglich der Header aller Blöcke geladen, dadurch wird nur ein Bruchteil an Speicherplatz benötigt. Das SPV Konzept ist ein Mechanismus zum Überprüfen, ob eine bestimmte Transaktion in der Blockchain enthalten und validiert ist, ohne die gesamte Blockchain durchsuchen zu müssen. Wie bereits beschrieben hat jeder Header einen Merkle Root, der aus der Transaktionsliste und den darin enthaltenen Transaktionen eines Blocks generiert wurde. Jede Transaktion hat also einen eigenen Hashwert, der über den Merkle Baum untrennbar mit dem Hashwert des Merkle Roots verbunden ist. Die Validierung erfolgt im SPV Konzept in zwei Schritten. Erstens wird überprüft, ob die Transaktion Teil des Blocks ist, und zweitens, ob der Block zur längsten und damit verifizierten Blockchain gehört. Es müssen wenigstens sechs weitere Blöcke validiert und der

Blockchain angefügt worden sein (Singhal et al., 2018, p. 210). Dieses Konzept macht es möglich, auch mit mobilen Geräten wie Smartphones oder Tablets Teil eines Blockchain Netzwerkes zu sein.

Das Prinzip der Blockchain ist eine Kombination aus drei Konzepten. Die Kryptografie sorgt für Transparenz und sichert zugleich Privatsphäre. Die Consensus Rules legen die Regeln fest um Konsens zu erzeugen und P2P-Netzwerke bilden die Grundlage zur Kommunikation der Teilnehmer.

2.3.3 Hashfunktion

Der Hashwert wird mittels der Hashfunktion berechnet. Die Hashfunktion transformiert mittels einer mathematischen Funktion eine beliebige Länge an Information in einen Wert, der aus Buchstaben und Zahlen besteht, in einer bestimmten Länge. Bei der SHA-256 Funktion ist die Länge mit 64 Zeichen definiert. Die Zahlen- und Buchstabenkombination besteht aus den Zahlen 0-9 und den Buchstaben A-F (als Ersatz für die Zahlen 10-15), das sogenannte Hexadezimal System (Czernik, 2016).

Die Hashfunktion hat folgende Eigenschaften (Drescher, 2017, p. 72ff.):

- Die Hashfunktion ist in der Lage, Hashwerte zu berechnen aus jeder Art von Daten input. Zudem führt die Berechnung schnell zu einem Ergebnis.
- Die Hashfunktion ist deterministisch, das bedeutet, dass identische Eingabedaten immer den gleichen Hashwert erzeugen. Abweichungen der Hashwerte dürfen ausschließlich durch veränderte Eingabedaten entstehen.
- Der Hashwert ist zufällig. Das bedeutet, dass sich der von der Hashfunktion ausgegebene Hashwert unvorhersehbar ändert, wenn die Eingangsdaten geändert werden. Auch wenn die Eingabedaten nur geringfügig geändert wurden, unterscheidet sich der resultierende Hashwert unvorhersehbar. Der Hashwert von geänderten Daten muss immer eine Überraschung sein. Es sollte nicht möglich sein, den Hashwert basierend auf den Eingabedaten vorherzusagen.
- Die Einwegfunktion bietet keine Möglichkeit, die Eingabewerte anhand des Ausgabewertes wiederherzustellen. Die eingegebenen Daten können also nicht anhand des ausgegebenen Hashwertes wiederhergestellt werden.
- Die Hashfunktion muss kollisionsresistent sein. Das bedeutet, dass unterschiedliche Eingabedaten nicht den gleichen Hashwert erzeugen können. Wobei dies nicht zu 100% ausgeschlossen werden kann sondern durch die Funktion eine derart geringe Wahrscheinlichkeit aufweist, dass man von einer Kollisionsresistenz sprechen kann.

Beispiel anhand des SHA-256 Verfahrens:

Eingabedaten: Unternehmen A überweist Unternehmen B die Summe 1000€

Hashwert: **8CFB7E48BECD678BCAD401487B1E4A119C1B07951204D84883844617CEE70C16**

Ändert sich die Information nur an einer Stelle, erhält man einen deutlich unterschiedlichen Wert.

Eingabedaten: Unternehmen A überweist Unternehmen B die Summe 100**1**€

Hashwert: **1E0E7A5B0872B26069F55FB9066C0E0F4FA96844FA588A0A2A7AA2C5639DB2F7**

In der Blockchain stellt der Hashwert des neuesten Blocks also immer den Wert aller bis dahin generierten Hashwerte dar. Durch die kleinste Änderung an einer Transaktion oder eines Blocks würde sich dieser Wert eindeutig ändern und sofort durch das Netzwerk erkannt werden. Gleichzeitig schließt das kryptografische Verfahren aus, dass man aus dem Hashwert Rückschlüsse auf die Eingabedaten ziehen kann. In dem Beispiel wurde zu Anschauungs-

zwecken ein einfacher Satz verwendet. Es ist wichtig anzumerken, dass alle Arten von Daten, also auch Programmcodes so verschlüsselt werden können. Dementsprechend auch Smart Contracts, die u.a. im Supply Chain Management eine wichtige Rolle spielen.

2.3.4 Kryptografie

Transaktionen werden also durch die Hashfunktion verschlüsselt. Damit die Daten einer Transaktion für Sender und Empfänger lesbar sind, gleichzeitig aber für Unberechtigte verschlüsselt bleiben, muss ein kryptografisches Verfahren verwendet werden, das dies gewährleistet. Die Blockchain verwendet dazu das sogenannte Asymmetrische Kryptosystem, bei dem für den Sender und Empfänger jeweils ein eigenes Schlüsselpaar verwendet wird. Jeder Schlüssel besteht dabei aus einem öffentlichen (Public Key) und einem privaten (Private Key) Schlüssel. Um das Prinzip zu verstehen, wird nun an einem einfachen Beispiel die Funktionsweise dargestellt, entnommen aus (Singhal et al., 2018, p. 78 ff.):

- Die Nachricht (m) von Alice wird mit der Hashfunktion (E) und dem Public Key von Bob (Puk_B) verschlüsselt zu einem Hashwert der durch den Public Key signiert wurde (c) und an Bob gesendet.
- Bob kann die verschlüsselte Nachricht (c) mit seinem Private Key (Prk_B) und der Funktion (D) entschlüsseln.

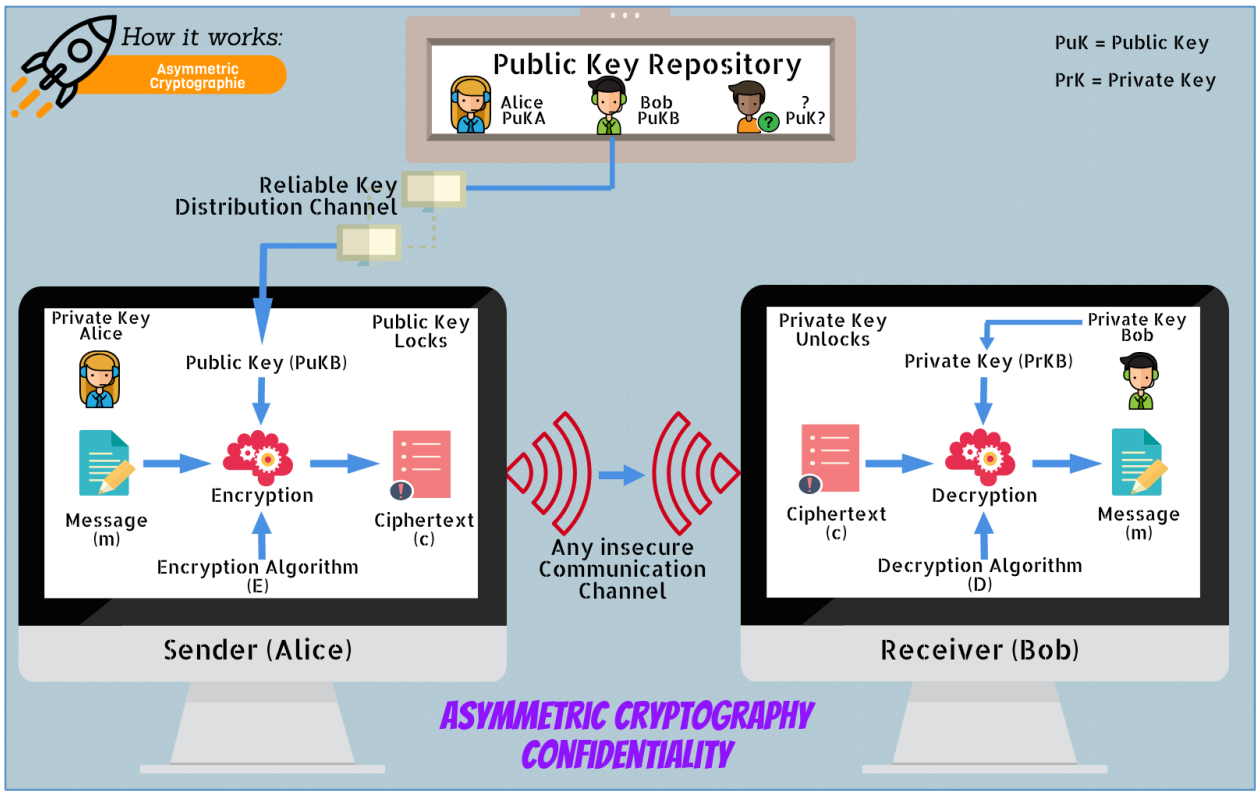

Abb. 17: Asymmetrisches Kryptoverfahren Vertrauenswürdigkeit, eig. Darstellung vgl. (Singhal et al., 2018, p. 79)

Der Public Key wird in einem öffentlichen Verzeichnis aufbewahrt, der Private Key sollte für Unberechtigte unzugänglich aufbewahrt werden. Das öffentliche Verzeichnis bietet dem Empfänger einer Nachricht die Möglichkeit, die Herkunft und Authentizität auf die gleiche Weise zu prüfen (Abb.17+18).

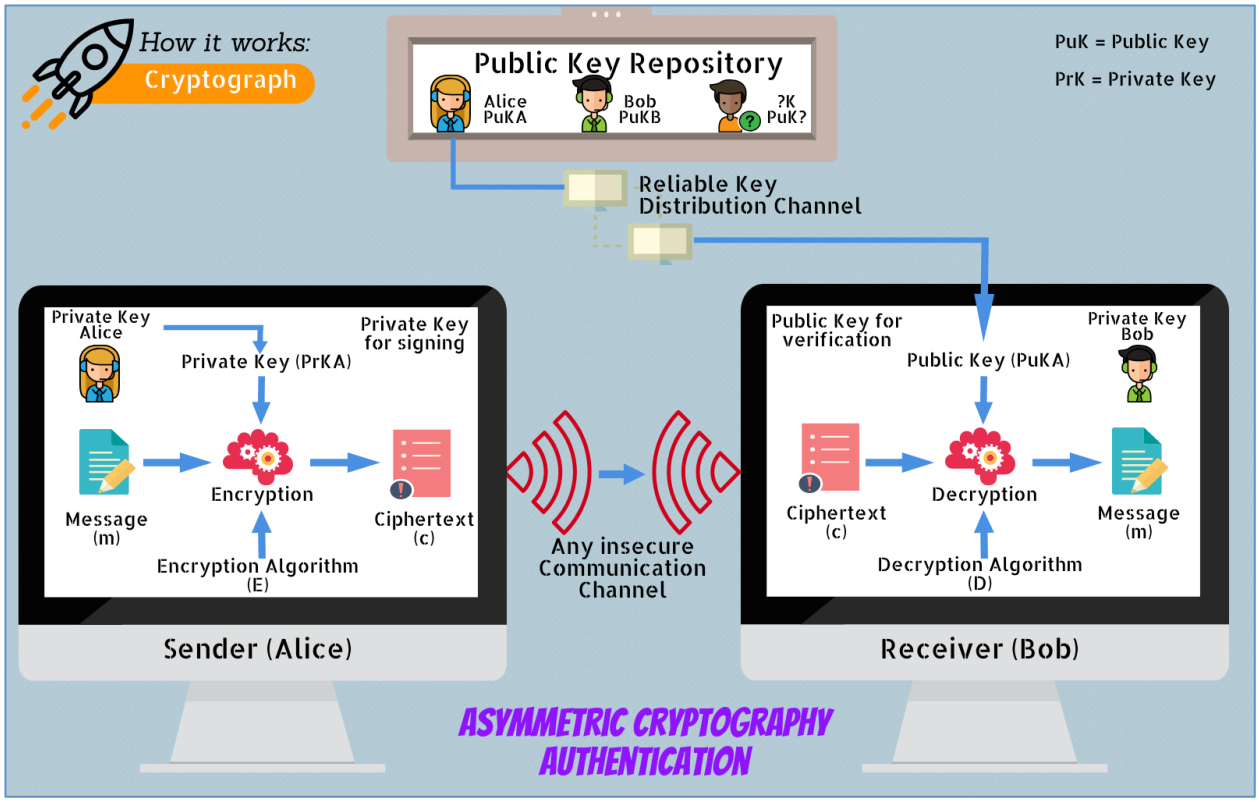

Abb. 18: Asymmetrisches Kryptoverfahren Authentizität, eig. Darstellung vgl. (Singhal et al., 2018, p. 79)

Durch die Signierung der Nachricht mit einem private Key erhält die Nachricht eine digitale Signatur.

Die NSA hat darauf aufbauend den Digital-Signature-Algorithm entwickelt. Das Prinzip ist in der folgenden Abbildung 19 darstellt.

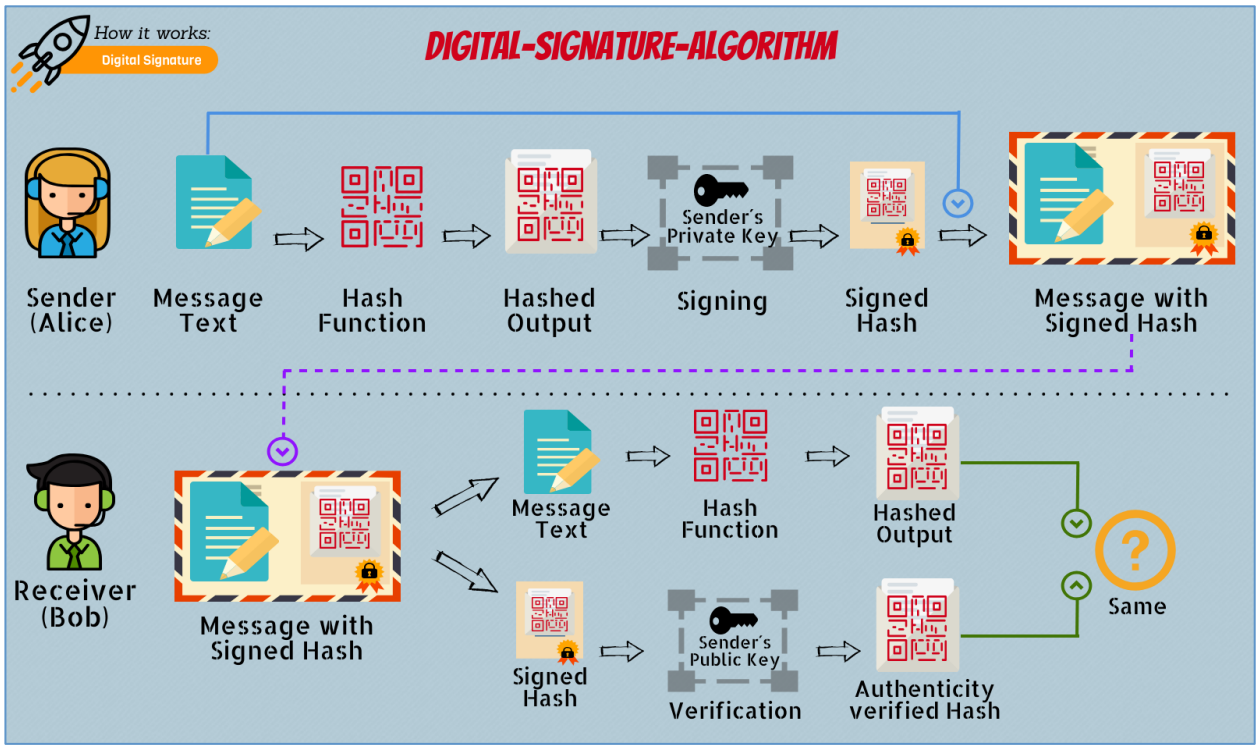

Abb. 19: Digital-Signature-Algorithm, eig. Darstellung vgl. (Singhal et al., 2018, p. 87)

Zuerst wird der Inhalt der Nachricht (oder Transaktion) durch die Hashfunktion verschlüsselt und anschließend der berechnete Hashwert mit dem Private Key signiert und als Cipher-Text ausgegeben. Dann wird die Nachricht gesendet, und der Empfänger kann die Herkunft durch den Public Key überprüfen und den Inhalt mit dem private Key entschlüsseln. Wenn die beiden Hashwerte am Ende übereinstimmen, ist die Authentizität bestätigt (Singhal et al., 2018, p. 87). Um eine Transaktion zweifelsfrei zu validieren wird also in der Blockchain die Hashfunktion als Nachweis der Authentizität der enthaltenen Informationen mit der Signatur als Nachweis des Senders angewendet.

Die Autorisierung von Transaktionen in der Blockchain, erfolgt durch das kryptografische Verfahren und die digitale Signatur. So werden folgende Anforderungen erfüllt (Drescher, 2017, p. 107):

- Der Sender einer Transaktion wird zweifelsfrei identifiziert und bestätigt, im Besitz der enthaltenen Daten zu sein. Das kann Kryptowährung sein oder sonstige Eigentumsrechte.
- Sie sind für den gesamten Inhalt der Transaktionsdaten einzigartig, um zu verhindern, dass sie ohne Zustimmung des Erstellers zur Genehmigung anderer Transaktionen verwendet werden.
- Allein der Sender kann die Signatur der Transaktion erstellen.
- Die Signatur muss einfach vom Netzwerk verifizierbar sein.

Die Schritte zum Signieren einer Transaktion nochmal zusammengefasst.

Eine Transaktion verschlüsseln und signieren (Drescher, 2017, p. 107):

1. Inhalt einer Transaktion genau beschreiben mit allen notwendigen Informationen.
2. Durch die Hashfunktion den Hashwert aus dem Inhalt der Transaktion berechnen.
3. Den Hashwert mit dem Private Key verschlüsseln.
4. Den Cipher-Text - generiert in Punkt 3 - der Transaktion als digitale Signatur anfügen.

Eine Transaktion überprüfen (Drescher, 2017, p. 108):

1. Den Hashwert der Transaktion ohne die Signatur generieren.
2. Entschlüsseln der digitalen Signatur der Transaktion mit dem öffentlichen Key des Senders. Und dann den Hashwert generieren.
3. Beide Hashwerte vergleichen. Stimmen sie überein, ist verifiziert, dass die Transaktion vom Sender autorisiert und nicht verändert wurde.

Dies war eine sehr vereinfachte Zusammenfassung und Darstellung des Themengebietes Kryptografie und sollte lediglich zum Verständnis des Blockchain Konzeptes dienen. Das Thema Kryptografie ist sehr komplex und kann hier nicht tiefergehend behandelt werden.

2.3.5 Consensus Rules

Um in einem Blockchain Netzwerk Konsens zu erzeugen gibt es mittlerweile verschiedene Konzepte. Das schon vorgestellte Proof of Work, welches in der Bitcoin Blockchain Anwendung findet, funktioniert seit Start des Netzwerkes absolut zuverlässig und konnte bis dato noch nicht gehackt werden. Welches Verfahren am besten geeignet ist, hängt von verschiedenen Faktoren ab. Handelt es sich um eine öffentliche oder private Blockchain? Wie hoch ist das Transaktionsvolumen und welche Skalierbarkeit wird gefordert?

2.3.5.1 Proof of Work

Proof of Work (PoW) wurde bereits in der Beschreibung des Grundprinzips der Blockchain ausführlich beschrieben. Um den korrekten Nonce zu finden, müssen sehr viele Werte ausprobiert werden. Dazu ist Rechenleistung erforderlich, die Energie benötigt. Je mehr Miner aktiv sind, desto höher wird das Difficult Target gesetzt. Dementsprechend wird mehr Rechenleistung benötigt, einen Block validieren zu können und die Belohnung in Form von Tokens zu erhalten. Dieses System stellt sicher, dass man Tokens nur erhalten kann, wenn man im Gegenzug Rechenleistung und die damit verbundenen Energiekosten einsetzt. In diesem System lohnt es sich nicht zu betrügen, sondern den Regeln entsprechend zu handeln.

In Abbildung 20 ist anschaulich dargestellt, was ein Angreifer leisten müsste, um eine Blockchain zu kompromittieren. Um erfolgreich zu sein, müsste der Angreifer mindestens 51% der Rechenleistung des gesamten Netzwerks erbringen, um erfolgreich einen Angriff durchführen zu können. Es kann davon ausgegangen werden, dass der Aufwand für Hardware und Energiekosten den potenziellen Gewinn durch einen Angriff übersteigt und somit nicht sinnvoll wäre. Die Webseite btc-echo.de kommt in einer stark vereinfachten Berechnung auf einen Wert von ca. 370 Milionen Euro, um eine 51% Attacke auf die Bitcoin Blockchain auszuführen (Kops, 2016).

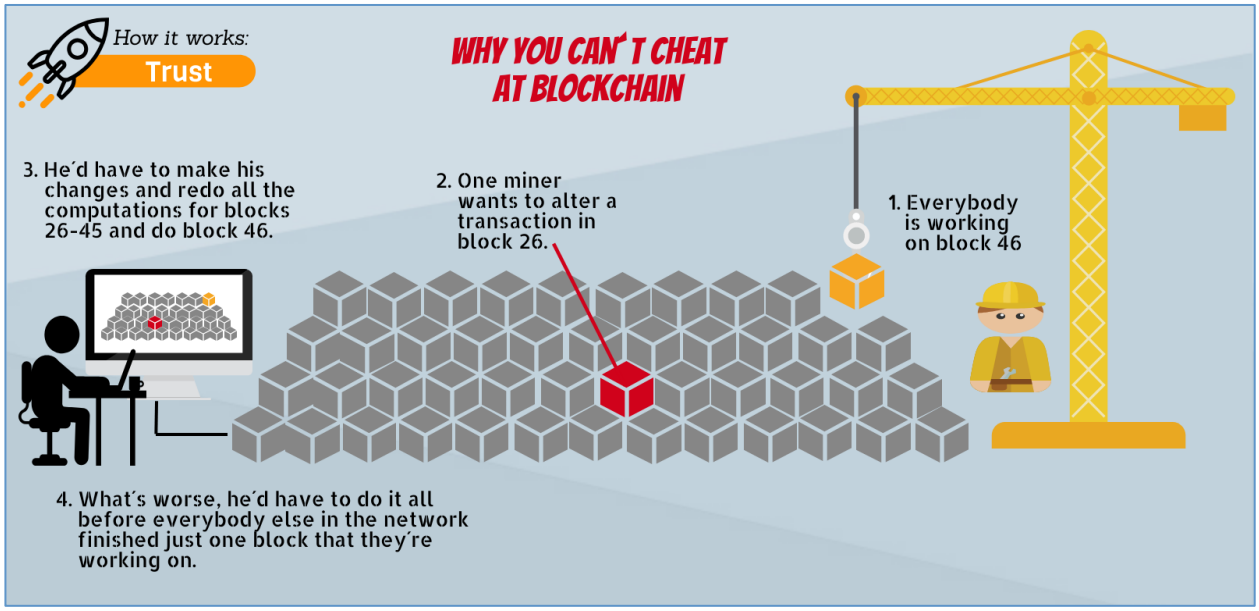

Abb. 20: Why you can´t cheat, eig. Darstellung vgl. (Konstantopoulos, 2017)

2.3.5.2 Proof of Stake

Proof of Stake (PoS) ist eine alternative Methode, um in einem Blockchain Netzwerk dezentralen Konsens zu schaffen. Anstatt wie bei PoW durch den Einsatz von Rechenleistung einen Wert zu erraten, entscheidet bei PoS die Höhe des eingesetzten Anteils an Token (Stake), wer den nächsten Block validieren darf. Hier spricht man nicht mehr vom Mining sondern vom Validieren, denn bei PoS muss kein Wert gefunden werden und es werden beim Validieren eines Blocks keine Tokens erzeugt und als Belohnung ausgegeben. Dennoch wird umgangssprachlich weiter vom Miner und mining gesprochen. Der Validierer (Miner) eines Blocks erhält lediglich Transaktionsgebühren in Form von Tokens. Entscheidend ist der eingesetzte Bestand an Tokens der Blockchain. In PoS-Systemen muss ein Miner den Anteil seines Tokenbestandes binden (das bedeutet, er kann diesen Anteil nicht für andere Zwecke einsetzen oder weitergeben) den er zum Validieren von neuen Blocks einsetzen möchte. Die Wahrscheinlichkeit, einen neuen Block validieren und erstellen zu können, ist proportional zu seinem Einsatz; je höher der eingesetzte Bestand, desto größer ist die Chance, einen neuen Block zu validieren und Transaktionsgebühren dafür zu erhalten. Ein Miner muss belegen, dass er einen bestimmten Prozentsatz aller zu einem bestimmten Zeitpunkt in einem bestimmten Währungssystem

verfügbaren Tokens besitzt. Wenn ein Miner zum Beispiel 2% des gesamten Ethers (ETH) im Ethereum-Netzwerk besitzt, kann er 2% aller zu validierenden Blöcke erstellen und dafür entsprechend Transaktionsgebühren erhalten (Singhal et al., 2018, p. 133).

Im Gegensatz zu PoW wird also keine Energie durch die Bereitstellung von Rechenleistung benötigt. Dadurch, dass der Validierer eines Blocks deterministisch bestimmt wird, können Transaktionen wesentlich schneller als bei PoW validiert und zu neuen Blöcken zusammengefasst werden. Bei PoS werden wie erwähnt keine Tokens durch den Mining Prozess erzeugt, deshalb werden in diesem System alle Tokens zum Start des Netzwerkes in einer fixen Menge erzeugt.

2.3.5.3 Delegated Proof of Stake

Delegated Proof of Stake (DPoS) nutzt ein Reputationssystem und Echtzeit-Abstimmungen, um einen Konsens zu erzielen. Es werden Repräsentanten durch die Netzwerkteilnehmer gewählt. Jeder Teilnehmer kann entsprechend seines Token Bestandes Stimmen verteilen, wobei die Stimmen jederzeit neu vergeben werden können. Aus dem sich dadurch ergebenden Ranking entsteht die Reihenfolge, die zum Validieren eines Blockes berechtigt und dafür Entlohnung in Form von Tokens zu erhalten. Repräsentanten, die für die Erstellung von Blocks verantwortlich sind, können Transaktionsdetails nicht ändern. Sie können jedoch verhindern, dass bestimmte Transaktionen in den nächsten Block aufgenommen werden. Allerdings verdoppelt sich die Dateigröße aufgeschobener Blöcke oder Transaktionen. Auf diese Weise wird verhindert, dass Repräsentanten in der Lage wären, das Netzwerk zu blockieren (Voshmgir and Kalinov, 2017, p. 19).

Repräsentanten, die in irgendeiner Form negativ auffallen, werden durch das Netzwerk durch Entzug der Stimmen als Repräsentant abberufen und können somit nicht mehr am Validieren von Blöcken partizipieren. Die Einnahmen, die ein Repräsentant durch das Validieren von Blöcken macht, können für verschiedene Zwecke eingesetzt werden. Es gibt auch Repräsentanten, die um Stimmen werben, indem sie die Einnahmen an die Wähler zu einem Teil auszahlen. Der DPoS gilt als effizientester, dezentralster, schnellster und flexibelster Konsensmechanismus. Theoretisch können 15.000 Transaktionen alle 15 Sekunden validiert werden (Malicek, 2018).

2.3.5.4 Proof of Burn

Proof of Burn (PoB) ist eine Alternative zu Proof of Work und Proof of Stake. Die Idee ist, dass die Miner den Beweis erbringen sollen, dass sie einen Teil ihrer Token „verbrannt" haben, d.h. an eine nachweislich nicht verwendbare Adresse geschickt haben. Dies ist aus individueller Sicht teuer, wie der Strombedarf bei PoW, verbraucht aber keine anderen Ressourcen außer den verbrannten Tokens. Wer Token verbrennt, erhält das Recht neue Blöcke validieren. Ähnlich wie bei Proof of Stake, steigt auch hier die Wahrscheinlichkeit für den nächsten Block ausgewählt zu werden, mit der Anzahl der Token, die man verbrannt hat. Um Token zu verbrennen werden diese an eine Adresse gesendet, die keinen Private Key besitzt und dadurch nicht rückwärts berechnet werden kann. So wird ausgeschlossen, dass man auf diese Tokens je wieder zugreifen kann (Voshmgir and Kalinov, 2017, p. 20).

2.3.5.5 Proof of Authority

Proof of Authority (PoA) ist ein Konsensmechanismus der in einer privaten Blockchain angewendet werden kann. Nodes müssen autorisiert sein um Zugang zum Konsensmechanismus zu erhalten. Die Netzwerkteilnehmer legen eine Anzahl an „ Authorities" fest und vergeben die Rechte zum Validieren eines Blocks an diese autorisierten Nodes. Konsens wird also nur unter einer begrenzten Anzahl an Nodes geschaffen. Das Validieren neuer Blocks erfolgt dabei rundenbasiert, bei dem in jeder Runde ein Node zum Miner gewählt wird, der dann einen neuen Block zum Validieren vorschlägt. Dieser neue Block muss anschließend von der Mehrheit der Authority Nodes bestätigt werden. Die Rechte zum Schreiben und Sichern der Blockchain sind dabei in der Regel identisch mit realen, physischen

Autoritäten, die folglich auch zur Rechenschaft gezogen werden können. So könnte ein gehackter Authority Node nicht einfach das Netzwerk übernehmen da er sofort identifiziert werden würde (Zeiselmair et al., 2018, p. 42).

Dieses Konzept widerspricht in Teilen dem dezentralen Grundgedanken der Konsensbildung bietet aber in privaten Blockchains Vorteile. Es ist keine hohe Rechenleistung notwendig wie bei PoW und bietet daher eine deutliche höhere Performance und ist dennoch sicherer als zentralisierte Datenbankprozesse (Zeiselmair et al., 2018, p. 42).

2.3.6 Peer-to-Peer

Peer-to-Peer (P2P) Systeme bestehen aus einem Netzwerk an eigenständigen Computern, die jeweils als Peer bezeichnet werden. Peer kann dabei gleichgesetzt werden mit Node. Da im Bezug zur Blockchain meistens von Nodes die Sprache ist wird im weiteren Verlauf ebenfalls der Begriff Node verwendet. Jeder Node stellt seine Rechenressourcen in Form von Speicherkapazität, Rechenleistung oder als Node zur Informationsverteilung zur Verfügung. Um an einem P2P-System teilzunehmen muss der Computer als ein Node agieren und Ressourcen zur Verfügung stellen, die Rollen und Rechte der Nodes sind dabei für jeden gleich.

Die drei wesentlichen Eigenschaften eines P2P-Systems sind (Schoder and Fischbach, 2002):

1. Client- und Serverfunktion. Jeder Node kann sowohl als Client als auch als Server agieren, wobei alle Nodes gleichberechtigt sind.
2. Kommunikation und Datenaustausch zwischen den Nodes findet direkt statt. Es gibt keine zentrale Instanz, die zwischengestaltet die Kommunikation koordiniert.
3. Jeder Node kann vollkommen autonom handeln und entscheiden, in welchem Umfang er Ressourcen zur Verfügung stellt.

P2P-Netzwerke sind also dezentral organisierte Systeme, die in Reinform ohne eine zentrale Stelle, die als Vermittler auftritt, auskommt. Bekanntes Beispiel war die Filesharing Plattform Napster, über die Daten direkt getauscht werden konnten. Napster war allerdings ein sogenanntes centralized P2P-System der ersten Generation, siehe Abbildung 21. Man hatte bei Napster keinerlei Sicherheit, dass man auch die Daten erhielt, die man wollte. Man konnte nicht kontrollieren, ob man beim Download einer MP3 Datei auch nur die Daten des gewünschten Musiksongs erhielt oder ob noch Schadsoftware enthalten war. Vertrauenswürdigkeit und Integrität wurden nicht durch Napster gewährleistet oder garantiert. Napster stellte sozusagen nur das Verzeichnis an Nutzern zur Verfügung und berief sich darauf lediglich als Vermittler von Nutzern aufzutreten und keine Haftung für Inhalte zu übernehmen. Ein reines P2P-System bietet alle Vorteile der Dezentralisation, allerdings ohne Vertrauenswürdigkeit und Integrität zu bieten.

Herausforderungen von P2P-Netzwerken sind (Prinz and T.Schulte, 2017, p. 17):

- Nodes eines P2P-Netzwerk können unterschiedliche Ziele verfolgen und versuchen, durch Manipulation Einfluss auf das Netzwerk zu ihren Gunsten zu nehmen.
- Fehlerhafte Informationen oder Softwarefehler können sich sehr schnell unbemerkt über das P2P-Netzwerk verbreiten. Ebenso wie bei Manipulationsversuchen ist eine aufwendige Überwachung und Detektierung notwendig.
- Viele Anwendungen erfordern eine Sicherstellung, dass Transaktionen vollständig und einmalig ausgeführt werden. Z.B. muss sichergestellt werden, dass Kryptowährung nicht mehrfach ausgegeben werden kann.

Die Blockchain löst diese Probleme und kann als Werkzeug zur Erreichung und Aufrechterhaltung der Integrität in dezentral organisierten P2P-Systemen betrachtet werden. Rein dezentral organisierte P2P-Systeme können die Blockchain nutzen, um die Systemintegrität zu erreichen und zu erhalten. Das Bindeglied zwischen P2P-Systemen und der Blockchain ist daher ihre Verwendung zur Erreichung und Aufrechterhaltung der Integrität (Drescher, 2017, p. 23).

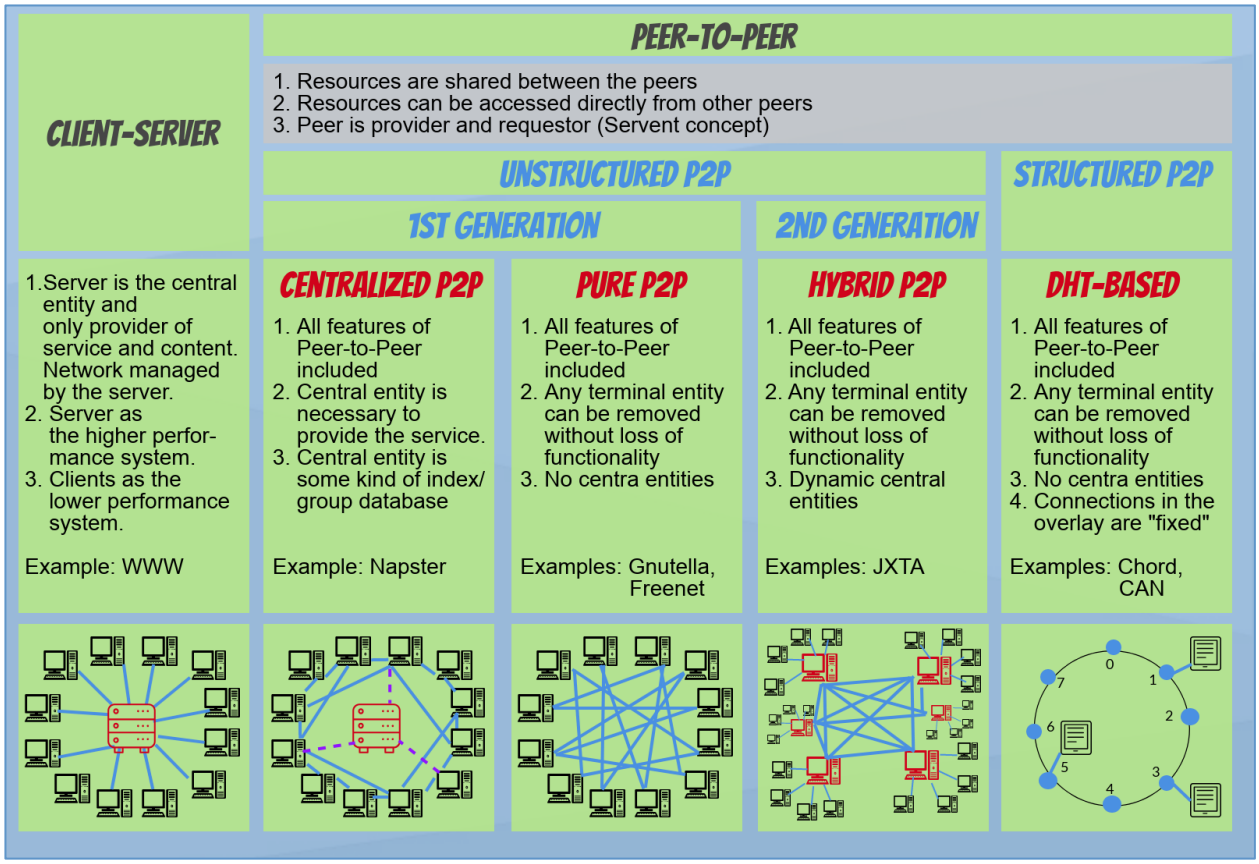

Abb. 21: Peer-to-Peer, eig. Darstellung vgl. (Eberspächer and Schollmeier, 2005)

2.3.7 Private vs. öffentliche Blockchain

Das Blockchain Konzept propagiert im Grunde den zugangsfreien Zutritt zum Netzwerk für jeden. Für öffentliche Blockchains wie Bitcoin, als reine Transaktionsplattform für Kryptowährung, ist das auch sinnvoll, da der Kerngedanke „Removing the Middleman" lautet. Für Unternehmen, die intern oder unternehmensübergreifend Blockchain in ihr Wertschöpfungsnetzwerk implementieren wollen, ist davon auszugehen, dass der Zugang zum Netzwerk auf die teilnehmenden Vertragspartner beschränkt sein soll, da Transaktionen zwar transparent und fälschungssicher für Netzwerkteilnehmer nachvollziehbar, nicht aber der Öffentlichkeit zugänglich sein sollen. Dies widerspricht dem Blockchain Prinzip dahingehend, dass zur Vergabe von Zugangsberechtigungen wieder eine dritte Stelle notwendig wird und Teilnehmer sich identifizieren müssen. Zugleich bietet diese Form einer Blockchain entscheidende Vorteile für Unternehmen, da private Blockchains leistungsfähiger sind und zugleich deutlich weniger Energie in Form von Rechenleistung benötigen.

Öffentliche Blockchains

Jeder kann am Netzwerk teilnehmen ohne Zugangsbeschränkungen. Der Programmcode ist Open Source, jeder kann ihn downloaden, installieren und als Node Transaktionen erstellen und validieren. Jeder Node kann theoretisch am Konsensbildungsprozess (Proof of Work), dem Minen von neuen Blöcken teilnehmen. Aufgrund der benötigten Rechenleistung, die steigt, je mehr Miner an dem Blockfindungsprozess arbeiten, wird es allerdings für die meisten Teilnehmer unrentabel, am Miningprozess teilzunehmen, da die Kosten des Energiebedarfs den Ertrag aus dem Minen neuer Blöcke übersteigt. Jede Transaktion kann öffentlich eingesehen werden, Transaktionen sind somit transparent aber dennoch anonym. Die Validierung von Transaktionen benötigt relativ viel Zeit, z.B. Bitcoin = 10 Minuten.

Konsortium Blockchains

Konsortium Blockchains operieren unter der Leitung einer Gruppe. Im Gegensatz zu öffentlichen Blockchains ist der Prozess zur Überprüfung von Transaktionen nicht für jeden zugänglich. Konsortium Blockchains sind schneller und haben eine höhere Skalierbarkeit. Der Konsensfindungsprozess wird durch eine vorab ausgewählte Gruppe von Nodes gesteuert und durch Mehrheitsfindung Konsens gebildet (PoA). Wenn bspw. ein Konsortium aus 20 Unternehmen besteht, wird Konsens erreicht, wenn 15 davon einen neuen Block validieren und somit für gültig erklären. Das Recht Transaktionen einzusehen, kann öffentlich oder auf die Teilnehmer beschränkt sein (Voshmgir and Kalinov, 2017, p. 14).

Private Blockchains

Schreibrechte werden zentral vergeben und verwaltet, Leserechte können öffentlich oder beliebig eingeschränkt vergeben werden. Beispiele für mögliche Anwendungen sind das Datenbankmanagement oder die Auditierung, die unternehmensintern oder netzwerkintern sein sollen, sodass eine öffentliche Lesbarkeit in vielen Fällen nicht erforderlich oder erwünscht ist. Im öffentlichen Sektor kann allerdings gerade die Fähigkeit zur öffentlichen Auditierung erwünscht sein. Private Blockchains sind eine Möglichkeit, die Vorteile der Blockchain-Technologie zu nutzen, indem Gruppen und Teilnehmer definiert werden, die Transaktionen intern validieren und dokumentieren. Dadurch sind sie wie in einem zentral organisiertem System dem Risiko der Manipulation ausgesetzt, da im Gegensatz zu öffentlichen Blockchains private Blockchains nicht durch Anreizmechanismen gesichert werden. Insbesondere wenn es um Skalierbarkeit und staatliche Einhaltung von Datenschutzbestimmungen und anderen regulatorischen Fragen geht, finden private Blockchains ihre Anwendung (Voshmgir and Kalinov, 2017, p. 14).

Netzwerk Typ	**Öffentlich**	**Konsortium**	**Privat**
Teilnehmer	Jeder	Zugangsberechtigte	
	Anonym	Identifiziert und Vertrauenswürdig	
Konsens Mechanismus	Mining Proof of Work	Abstimmung / Multi Parteien Konsens Algorithmus Proof of Stake	
	- großer Energiebedarf - keine Endgültigkeit - 51% Angriffsmöglichkeit	- Leichter & Schneller - geringer Energiebedarf - Ermöglicht Endgültigkeit	
Transaktions-bestätigungsfrequenz	Lang (Bitcoin z.B. 10 Min)	Kurz (100x msec)	
Anwendungsfeld	Kryptowährung	Transaktionsplattform im Geschäftsbereich, z.B. Supply Chain Networks	

Tab. 1: Vergleichsmatrix Konsensfindungs Ansätze, eig. Darstellung vgl. (Tamayo, 2017, p. 21)

Für eine Anwendung der Blockchain Technologie in Wertschöpfungsnetzwerken werden weitestgehend private Blockchains implementiert werden. Sie sind leistungsfähiger, und jeder Teilnehmer ist bekannt und vertrauenswürdig. Die notwendige Authentifizierungsstelle widerspricht in Teilen dem Blockchain Konzept, bringt aber wie beschrieben Vorteile für Unternehmen.

2.4 Stand der Blockchain Entwicklung

Die Unternehmensberatung Gartner erstellt regelmäßig sogenannte Hype Cycles zu verschiedenen Themenbereichen. Der Hype Cycle soll veranschaulichen, wie ausgereift eine Technologie ist und in welchem Stadium der Entwicklung sie sich befindet. Unternehmen können daraus grob ableiten, wann neue Technologien relevant werden könnten und wann der Einstieg des eigenen Unternehmens sinnvoll sein könnte.

Der Hype Cycle wird dabei in fünf Phasen unterteilt (Gartner, 2018):

1. **Innovation Trigger:** Ein möglicher technologischer Durchbruch ist der Innovationstreiber. Frühe Proof-of-Concept-Storys und das Medieninteresse sorgen für eine hohe Aufmerksamkeit. Oftmals gibt es keine verwendbaren Produkte, und die wirtschaftliche Rentabilität ist nicht nachgewiesen.
2. **Peak of Inflated Expectations:** Frühe Veröffentlichungen produzieren eine Reihe von Erfolgsgeschichten - oft begleitet von zahlreichen Misserfolgen. Einige Unternehmen ergreifen Maßnahmen, andere nicht.
3. **Trough of Disillusionment:** Das Interesse nimmt ab, da Experimente und Implementierungen nicht erfolgreich sind. Die Produzenten der Technologie wackeln oder scheitern. Die Investitionen gehen nur dann weiter, wenn die verbleibenden Anbieter ihre Produkte zur Zufriedenheit der Early Adopters verbessern.
4. **Slope of Enlightment:** Weitere Anwendungsbeispiele, wie die Technologie dem Unternehmen zugutekommen kann, beginnen sich zu kristallisieren und werden besser verstanden. Produkte der zweiten und dritten Generation kommen von Technologieanbietern. Mehr Unternehmen finanzieren Pilotprojekte, konservative Unternehmen bleiben zurückhaltend.
5. **Plateau of Productivity:** Die Einführung der Mainstream-Technologie beginnt zu wachsen. Die Kriterien für die Beurteilung der Rentabilität von Anbietern sind klarer definiert. Die breite Markttauglichkeit und Relevanz der Technologie zahlt sich deutlich aus.

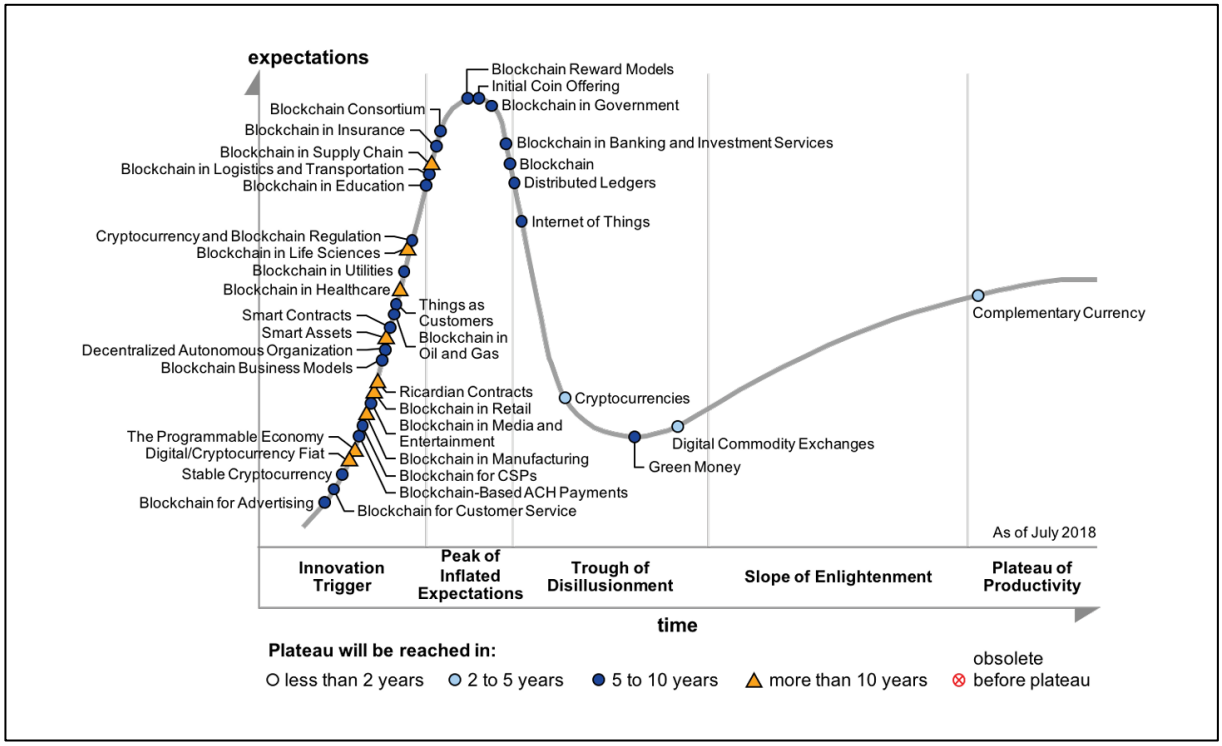

Abb. 22: Gartner Hype Cycle for Blockchain Business 2018, Quelle (Pemberton Levy, 2018)

Der Gartner Hype Cycle for Blockchain Business (Abb.22) verdeutlicht den Umstand, dass die Blockchain Technologie sich als Ganzes am Ende des Hypes, also der Phase zwei befindet und Kryptowährungen kurz vor der Talsohle der

Ernüchterung stehen. Gut erkennbar ist allerdings, dass konkrete Anwendungsgebiete wie in der Supply Chain, im Manufactoring oder im Customer Service noch am Anfang stehen und als Technologien mit potenziellem Durchbruchscharakter ihre Anwendbarkeit und wirtschaftliche Rentabilität beweisen müssen. Wesentlichen Anteil daran hat die Ethereum Blockchain, die, im Gegensatz zur Bitcoin Blockchain, entwickelt wurde, um weitergehende Anwendungen auf ihr programmieren zu können.

2.4.1 Ethereum

Während die Bitcoin Blockchain ausschließlich als Transaktionsplattform für die Kryptowährung Bitcoin fungiert, ist die Ethereum Blockchain frei programmierbar für Anwendungen, die in vielen Bereichen einsetzbar sind. Vor allem das Konzept der Smart Contracts bietet interessante Möglichkeiten in Wertschöpfungsnetzwerken. Ethereum nutzt ebenfalls ein dezentral organisiertes P2P-Netzwerk als Grundlage. Ethereum nutzt wie die Bitcoin Blockchain Proof of Work als Konsensbildungsmodell, aufgrund des hohen Energiebedarfs wird momentan daran gearbeitet, die Ethereum Blockchain auf Proof of Stake umzustellen.

Der innovative Ansatz der Ethereum Blockchain ist das Implementieren eines Abstraction Layers (Abb.23). Dadurch wird es möglich, Transaktionen verschiedener Anwendungen durch einen generalisierten Programmcode auf allen Nodes laufen zu lassen (Singhal et al., 2018, p. 221).

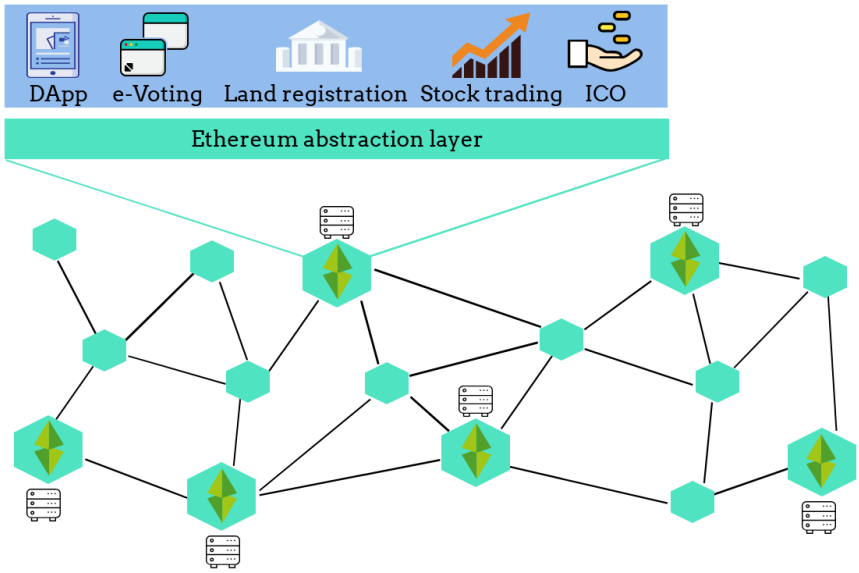

Abb. 23: Multiple Anwendung auf Ethereum, eig. Darstellung vgl. (Singhal et al., 2018, p. 221)

Die Datenstruktur eines Blockes unterscheidet sich dahingehend, dass nicht nur ein Merkle Root im Header enthalten ist sondern drei Merkle Roots (Singhal et al., 2018, p. 225):

- **State Root**: repräsentiert den aktuellen Stand der Blockchain im Netzwerk.
- **Transactions Root**: entspricht dem Merkle Root der Bitcoin Blockchain, also der Hashwert generiert durch die im Block enthaltenen Transaktionen.
- **Receipts Root**: Hashwert aus den Empfangsbelegen der im Block enthaltenen Transaktionen.

In der Ethereum Blockchain werden die Teilnehmer in Accounts eingeordnet (Dhillon et al., 2017, p. 28):

- **User Accounts:** Werden auch als externe Accounts bezeichnet. Diese Accounts werden von Anwendern gesteuert und Transaktionen durch das public-private Schlüsselpaarverfahren kontrolliert. Alle Aktionen im Netzwerk werden durch Transaktionen ausgelöst, die von User Accounts initiiert werden. In der Bitcoin Blockchain werden User Accounts einfach als Adressen bezeichnet. Der Unterschied zwischen Accounts und Adressen besteht in der Möglichkeit, dass Accounts in Ethereum generalisierten Code enthalten und ausführen können.
- **Contract Accounts:** Der Account wird durch einen eigenen Code gesteuert. Contracts sind die funktionale programmatische Einheit der Ethereum Blockchain. Der Account hat einen zugehörigen Code und kann den Code ausführen, wenn er durch Transaktionen ausgelöst wird, die von anderen Accounts empfangen wurden. Er kann seinen eigenen Speicher modifizieren. Jeder Contract in der Blockchain hat seinen eigenen Speicher, den nur er selbst beschreiben kann; dies wird als State des Contract bezeichnet. Jeder User im Netzwerk kann eine Anwendung mit bestimmten Regeln erstellen und sie als Contract definieren.

In der Bitcoin Blockchain werden validierte Transaktionen fortgeschrieben und sind in den Blöcken enthalten. Der daraus folgende, aus dem Header abgeleitete Hashwert des zuletzt angefügten Blocks repräsentiert den aktuell gültigen Stand der Blockchain. In der Ethereum Blockchain wird vom State (Zustand) gesprochen. Das bedeutet, dass die States aller Accounts in Kombination mit den Account Adressen den sogenannten World State repräsentieren, also den aktuell gültigen Zustand der Ethereum Blockchain (Wood, 2018, p. 3). Die Änderung des Zustandes eines Accounts wird immer durch eine entsprechende Transaktion protokolliert. In der Ethereum Blockchain werden also nicht einfach Transaktionen gespeichert, sondern die Änderungen der Accounts. Wird in der Bitcoin Blockchain bspw. bei einer Transaktion lediglich ein Betrag an Bitcoins von der Senderadresse an die Empfängeradresse protokolliert, wird in der Ethereum Blockchain die Änderung des Bestands an Ether (beim Sender - / beim Empfänger +) des jeweiligen Accounts protokolliert.

Der Account State besteht aus vier Bereichen (Wood, 2018, p. 3):

- **Nonce:** Wert, der der Anzahl von dieser Adresse gesendeten Transaktionen entspricht, oder im Falle von Accounts mit zugehörigem Code der Anzahl der von diesem Account erstellten Smart Contracts.
- **Balance:** Wert, der der Anzahl an Ether entspricht, die der Account besitzt.
- **Storage Root:** 256-Bit-Hashwert des Merkle Roots eines Merkle Trees, der die gespeicherten Daten des Accounts kodiert.
- **Code Hash:** Hashwert des EVM-Codes (Ethereum Virtual Machine). Dieser Code wird ausgeführt, wenn der Account einen Nachrichtenaufruf erhält. Dieser Wert wird einmalig vergeben und kann im Gegensatz zu allen anderen Bereichen nach der Account Erstellung nicht mehr geändert werden.

Wichtiges Differenzierungsmerkmal ist die Ethereum Virtual Machine (EVM), die die Entwicklung und Betreibung von sogenannten Decentralized Applications, kurz DApps, in unterschiedlichen Programmiersprachen ermöglicht.

Die EVM ist eine Runtime-Umgebung für Smart Contracts. Sie werden in der Programmiersprache Solidity geschrieben und dann mit Hilfe eines Interpreters in EVM zu Bytecode kompiliert. Dieser Bytecode wird dann über einen Ethereum Client in die Blockchain hochgeladen. In dieser ausführbaren Bytecode-Form können Smart Contracts dann durch Transaktionen ausgelöst werden. Die EVM ist so konzipiert, dass sie vollständig von der Umgebung und dem Rest des Netzwerks isoliert ist. Der in der EVM laufende Code hat keinen Zugriff auf das Netzwerk oder andere Prozesse. Erst nach der Kompilierung zu Bytecode haben Smart Contracts Zugriff auf das Netzwerk und andere Verträge. Aus operativer Sicht verhält sich das EVM wie ein großer dezentraler Computer mit Millionen von Objekten (Accounts), die in der Lage sind, eine interne Datenbank zu pflegen, Code auszuführen und miteinander zu kommunizieren. Die EVM ermöglicht es jedem Account im Netzwerk, beliebigen Code in einer sicheren Umgebung aus-

zuführen, in der das Ergebnis vollständig deterministisch ist und die Ausführung garantiert werden kann. Die standardmäßige Ausführungsumgebung und die Standardeinstellungen führen dazu, dass sich am State nichts ändert, solange bis ein User von einem externen Account aus eine Transaktion initiiert und dadurch eine Aktion auslöst. Diese Aktion kann zu zwei Ergebnissen führen: Wenn der Empfänger ein anderer externer Account (User Account) ist, dann wird durch die Transaktion Ether übertragen. Wenn der Empfänger jedoch ein Smart Contract ist, wird der Vertrag aktiviert und führt den darin enthaltenen Code aus (Dhillon et al., 2017, p. 33).

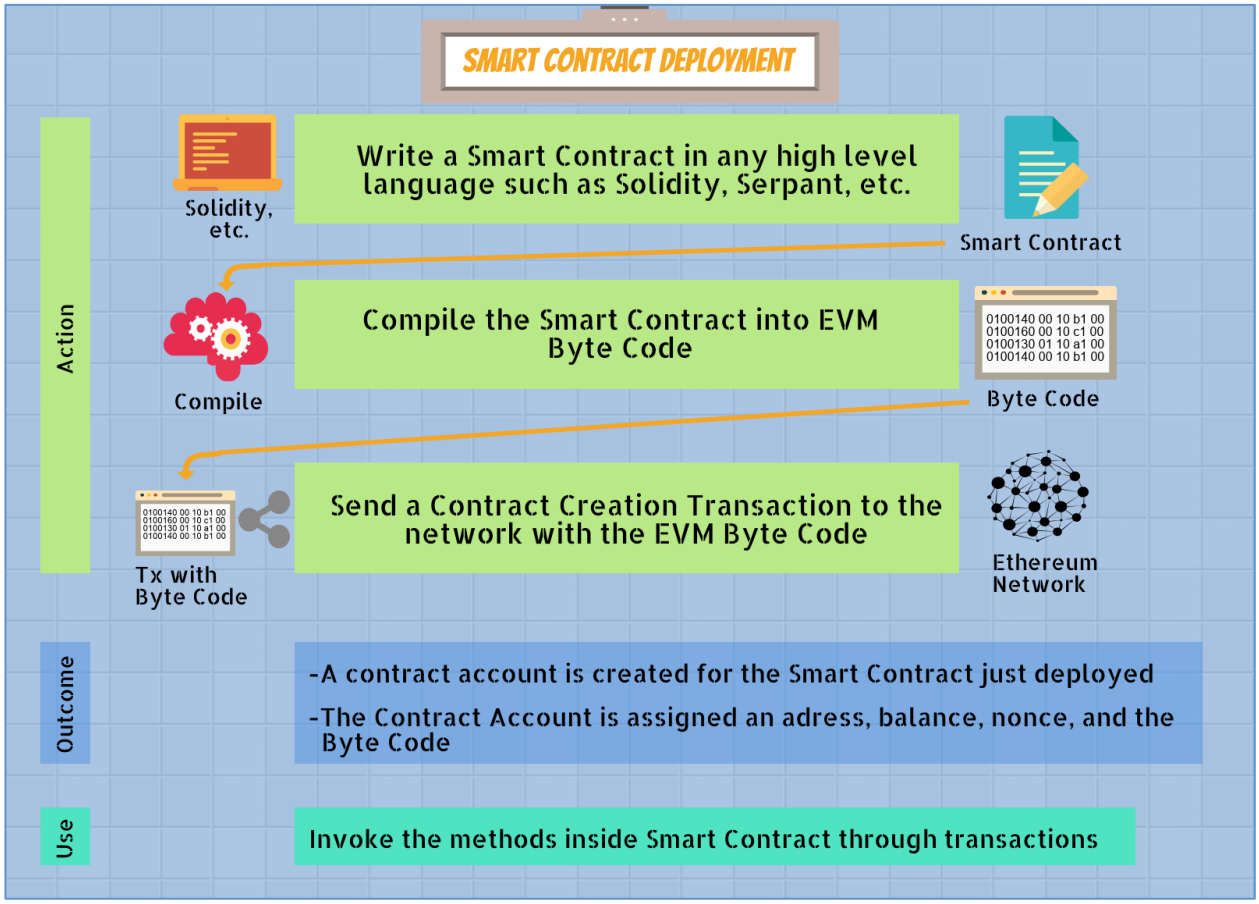

Abb. 24: Smart Contract deployment, eig. Darstellung vgl. (Singhal et al., 2018, p. 260)

3. Smart Contracts

Das Prinzip und der Begriff der Smart Contracts wurde bereits in den 1990ern durch Nick Szabo beschrieben, wonach digitale Werte direkt durch einen Code gesteuert und beliebig viele Regeln implementiert werden können. Ein Smart Contract ist demnach ein computergestütztes Transaktionsprotokoll, das Bedingungen eines Vertrages erfüllt. Smart Contracts sind also nicht gleichzusetzen mit vertraglichen Vereinbarungen. Allgemeine Ziele der Smart Contracts sind die Erfüllung festgelegter Vertragsbedingungen (wie bspw. Zahlungsbedingungen), unerwünschte Abweichungen zu vermeiden, und die Notwendigkeit von vertrauenswürdigen Vermittlern zu minimieren (Szabo, 1997).

Drei Schlüsselelemente unterscheiden Smart Contracts von herkömmlichen Verträgen (Swan, 2015, p. 10):

1. Autonomie: Sobald ein Smart Contract auf der Blockchain ausgeführt wurde, muss er nicht mehr mit seinem Initiator in Kontakt bleiben.
2. Selbstständigkeit: Ein Smart Contract hat die Fähigkeit, jede Art von Ressource selbstständig zu steuern. So könnte bspw. ein Smart Contract durch die Bereitstellung von Dienstleistungen oder die Ausgabe von Eigenkapital Mittel beschaffen und diese für die benötigten Ressourcen, wie beispielsweise die Speicherung von Rechenleistung, verwenden.
3. Dezentralisierung: Smart Contracts werden in Blockchains angelegt und sind so über das ganze Netzwerk verteilt und selbstständig ausführbar.

Industrie 4.0 und die Vernetzung zu cyber-physischen Systemen erfordern automatisierte Prozessabläufe in Wertschöpfungsnetzwerken. Bedarfe und Angebote sollen sich automatisch zu wertschöpfenden Prozessen verbinden, und die Anbahnung sowie der Abschluss von Geschäftsbeziehungen sollen ebenfalls automatisiert möglich werden (BMWi, 2017, p. 5). In der bereits erwähnten Forschungsagenda zu Industrie 4.0 des BMWi wurden dazu, unter anderem, Fragen formuliert, auf die das Konzept der Smart Contracts Antworten liefern kann:

- Wie können automatisiert Verträge zwischen Maschinen und Produkten einerseits und Produktionsaufträgen, Transportdienstleistungen, Wartungsaufträgen usw. andererseits geschlossen werden? Wie gestalten sich Vertragsanpassungen?
- Wie können und dürfen Maschinen Verträge abschließen? Klärung der Fragen zur juristischen Person und der Bezahlung.
- Wie befähigt man Anbieter, ihre angebotenen Leistungen formal zu beschreiben und zur Verfügung zu stellen?
- Wie kann sichergestellt werden, dass Verhandlungen über die Auftragsvergabe in Echtzeit und garantiert zum vereinbarten Zeitpunkt zu einem rechtssicheren Ergebnis führen? Wie können abweichende Ziele und Rahmenbedingungen, die zur Entwurfszeit unbekannt waren, berücksichtigt werden?

Die Frage nach dem „Wie" kann durch das Konzept der Smart Contracts beantwortet werden, wie im weiteren Verlauf beschrieben wird. Die Frage nach dem „Ob" Maschinen oder Softwareprogramme Verträge schließen dürfen, bedarf noch einer juristischen Klärung. Nach deutschem Recht ist Rechtsfähigkeit die Fähigkeit, selbstständig Träger von Rechten und Pflichten zu sein. Dabei ist die Rede von Rechtssubjekten. Träger sind dabei natürliche Personen, Juristische Personen und Personengesellschaften ("Rechtsfähigkeit (Deutschland)," 2018). Zu klären ist also, inwieweit Maschinen und Softwareprogramme Rechtssubjekte sein können und als Träger von Rechten und Pflichten rechtsfähig im Sinne des Gesetzes sind. Es wird bereits aufgrund der wachsenden Autonomie intelligenter Maschinen und Softwareprogramme über die Anerkennung einer E-Person mit eigener Rechtspersönlichkeit diskutiert, also elektronische Agenten, die eigenständig ohne menschliches Eingreifen Verträge auf Grundlage intelligenter Algorithmen abschließen. Darüber hinaus wird über eine Anpassung des Vertrags- und Haftungsrechts diskutiert (Sakowski, 2018, p. 29). In Deutschland sind Verträge grundsätzlich an keine Form gebunden, d.h. sie

können nach Wahl der Parteien mündlich oder schriftlich abgeschlossen werden. Es gibt allerdings Geschäfte, die durch Gesetz eine Form vorgeschrieben haben. Beispielsweise die Schriftform und notarielle Beurkundung bei Immobilienübertrag. Der Paragraph §126a BGB regelt die elektronische Form[8]. Inwieweit die elektronische Form Smart Contracts und den darin enthaltenen Programmcode umfasst, ist nicht Teil dieser Arbeit und muss juristisch an anderer Stelle geklärt werden.

3.1 Funktion Smart Contracts

Smart Contracts sind Programmcodes, die auf einer Blockchain laufen und ausführbar sind. Der Code enthält Bedingungen und Regeln, die zwei oder mehr Parteien vereinbart haben. Diese Computerprogramme beruhen vereinfacht betrachtet auf dem IF→THEN→ELSE Prinzip. In dem Whitepaper zum Hyperledger Projekt[9] werden Smart Contracts definiert als „*...self-executing agreements between parties that have all relevant covenants spelled out in code, are settled automatically, and can be dependent upon future signatures or trigger events.*" (Hyperledger Project, 2017).

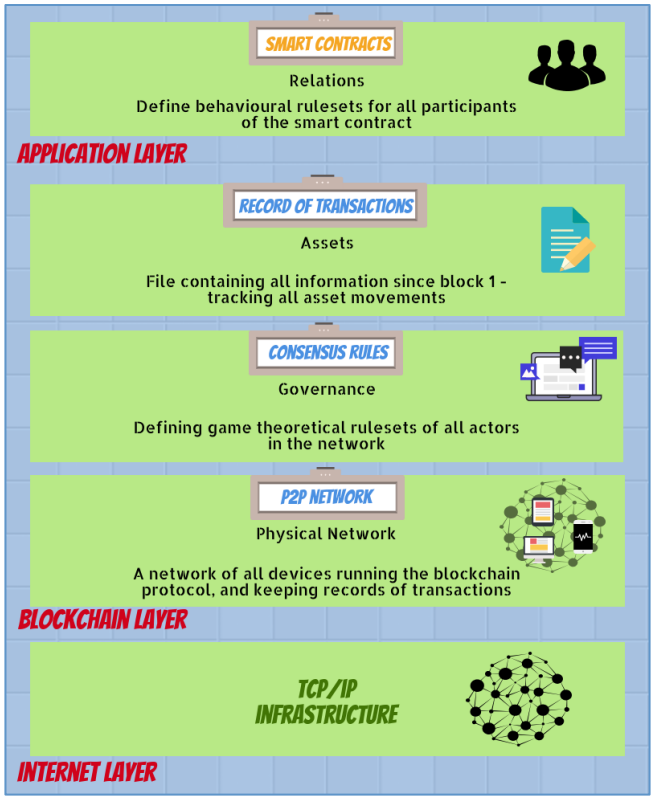

Abb. 25: Blockchain Layers, eig. Darstellung vgl. (Voshmgir and Kalinov, 2017, p. 7)

Wie bereits unter 2.4.1 beschrieben sind Smart Contracts Kern des Ethereum Blockchain Protokolls und spielen als Contract Accounts eine wesentliche Rolle. Ethereum entwickelte die Idee, die Vertragsebene (Contract Layer) von dem Blockchain Layer zu entkoppeln. Das Ledger wird von Smart Contracts verwendet um, bei Erfüllung bestimmter vordefinierter Bedingungen oder dem Eintreten bestimmter Ereignisse automatisch Transaktionen auszulösen. Die Entkopplung des Smart Contract Layer von dem Blockchain Layer ermöglicht eine flexible Entwicklungsumgebung (Voshmgir and Kalinov, 2017, p. 7).

[8] BGB §126a Elektronische Form (Deutschland and Köhler, 2018)

(1) Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur versehen.

(2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

[9] Hyperledger ist ein Open-Source-Projekt zur Weiterentwicklung branchenübergreifender Blockchain-Technologien. Es ist eine globale Zusammenarbeit mit führenden Unternehmen aus den Bereichen Bankwesen, Finanzen, Internet der Dinge, Fertigung, Lieferketten und Technologie (Hyperledger.org, 2018).

Smart Contracts sind also in der Lage, selbstständig Transaktionen auszulösen, wenn die im Code verankerten Bedingungen erfüllt sind. Er kann Geschäftsbeziehungen zwischen Personen oder Institutionen und dazu den Besitz an Vermögenswerte formalisieren. Die Transaktionsregeln des Smart Contract definieren die Bedingungen, Rechte und Pflichten, denen die Parteien zustimmen. Dieser Transaktionsregelsatz wird dann in digitaler Form formalisiert, also in einem maschinenlesbaren Code. Diese im Smart Contract festgelegten Rechte und Pflichten können nun automatisch von jedem Node innerhalb des Netzwerkes ausgeführt werden, sobald die im Code formalisierten Bedingungen erfüllt sind (Voshmgir and Kalinov, 2017, p. 24).

Smart Contracts können auch als eine Geschäftslogik betrachtet werden, die auf einer Blockchain implementiert ist und Transaktionen regelt und definiert. Smart Contracts können so simpel wie ein Datenupdate oder so komplex wie die Ausführung eines Vertrages mit verknüpften Bedingungen sein. So kann beispielsweise ein Smart Contract einfach nur einen Kontostand durch Validierung aktualisieren, um sicherzustellen, dass genügend Guthaben auf einem Konto ist, bevor eine Transaktion durchgeführt wird. Ein komplexerer Smart Contract kann bspw. Bedingungen enthalten, die Kosten für den Versand eines Produkts an den Liefertermin koppeln und Eigentumsübergang dann im Ledger dokumentieren und den Zahlungsvorgang auslösen (Hyperledger, 2018, p. 3).

Es gibt zwei verschiedene Arten von Smart Contracts (Hyperledger, 2018, p. 3):

- Installierte Smart-Contracts installieren die Geschäftslogik auf den Nodes im Netzwerk, bevor das Netzwerk aktiv wird.
- On-Chain-Smart-Contracts implementieren die Geschäftslogik durch eine Transaktion auf der Blockchain, die dann von nachfolgenden Transaktionen aufgerufen wird. Bei On-Chain Smart Contracts wird der Code, der die Geschäftslogik definiert, Teil des Ledgers.

In Ethereum werden Smart Contracts als eigenständige, zustandsbehaftete (state), adressierbare Objekte betrachtet, die durch den Erhalt einer Nachricht ausgelöst werden können, wodurch sich der Zustand des Vertrages ändert (Welzel et al., 2017, p. 14). Die Änderung des Zustandes eines Smart Contracts wird durch den State Root (siehe 2.4.1) repräsentiert und dokumentiert. Abbildung 26 veranschaulicht die Position eines Smart Contracts innerhalb eines Blockes. Wie bereits beschrieben bedeutet die Änderung auch nur eines Bytes eine Zustandsänderung die auf die gesamte Blockchain Auswirkung hat. Ändert sich also der Zustand eines Contracts, bspw. durch Auslösen eines im Vertrag festgelegten Ereignisses, muss diese Änderung des Zustandes validiert und vom Netzwerk akzeptiert werden.

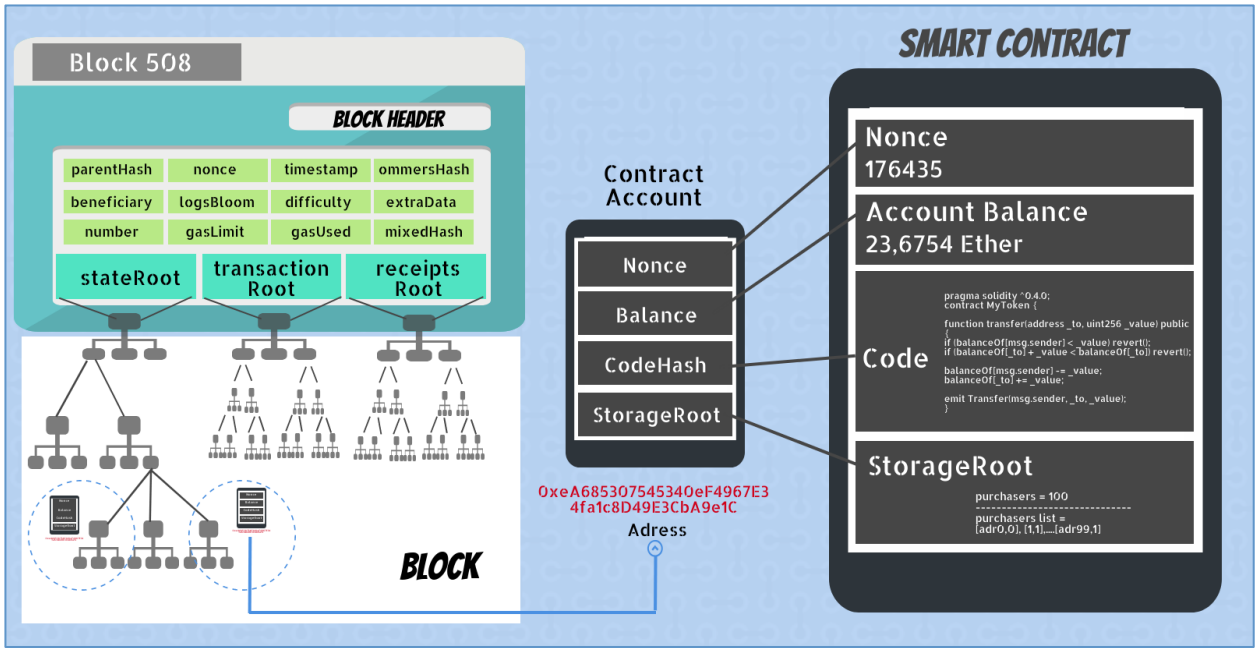

Abb. 26: Position Smart Contract innerhalb eines Blocks, eig. Darstellung vgl. (Singhal et al., 2018, p. 255)

Um sicherzustellen, dass nicht beliebig viele Transaktionen aufgerufen werden und dadurch das Netzwerk angegriffen wird, müssen bei Ethereum Smart Contracts ein gewisses Volumen an Gas (Gas Limit) enthalten, um die benötigte Rechenleistung für eine Transaktion zu limitieren. Durch den Gas Price kann man steuern, wie schnell eine Transaktion ausgeführt wird. Der Unterschied zwischen Ether und Gas wurde von (Welzel et al., 2017) treffend beschrieben:

> *„Da jede Operation (Addition, Daten speichern, Daten lesen, etc…) eines Smart Contract Rechenleistung der Blockchain verbraucht, wird dem Smart Contract ein maximales Volumen in Gas zugeordnet. Um den Unterschied zwischen Gas und Ether anschaulicher zu machen kann man sich ein Auto vorstellen. Damit es fährt, muss es mit Sprit betankt werden (hier Gas). Der Sprit wird in Euro bezahlt. Während der Spritverbrauch des Autos konstant ist, ist der Europreis pro Liter variabel. Analog wird der Preis pro Einheit Gas in Ether berechnet."* (Welzel et al., 2017, p. 14).

Gas Limit – legt den maximalen Betrag an Gas fest, den man bereit ist, für eine Transaktion auszugeben. Die benötigte Menge an Gas ergibt sich aus dem im Smart Contract enthaltenen Code. Dieser bestimmt wie viel Rechenleistung notwendig ist, den Code auszuführen. Es muss also mindestens so viel Gas dem Smart Contract zugefügt werden, um genug Rechenleistung abrufen zu können, die der enthaltene Code benötigt. Ist nicht genug Gas enthalten, wird die Transaktion aufgrund eines „out of gas" Error nicht durchgeführt (myetherwallet.com, 2018). Wenn die Menge an Gas, die benötigt wird, die einzelnen Schritte der Transaktion auszuführen, gleich groß oder kleiner wie das hinterlegte Gas Limit ist, wird die Transaktion durch einen Miner ausgeführt. Wenn das Gas Limit nicht ausreicht, also die Ausführung der Transaktion mehr Gas verbrauchen würde, läuft die Transaktion „out of gas", ist aber trotzdem valide und der Miner erhält den vollen Betrag des gesetzten Gas Limits. Verbraucht im Gegenzug die Transaktion nicht das hinterlegte Gas Limit, erhält man die Differenz zurück. Das Gas Limit für eine Standard Transaktion ist 21.000. Wenn man bspw. 100.000 als Gas Limit festgelegt hat und die Transaktion nur 21.000 Gas verbraucht, erhält man 79.000 Gas zurück.

Gas Price – legt fest wie schnell eine Transaktion ausgeführt wird.

Die Gebühren einer Transaktion ergeben sich aus dem verbrauchten Gas Limit x Gas Price und muss bei der Initiierung einer Transaktion vollständig bezahlt werden. Wird nicht die gesamte Menge Gas verbraucht, erhält man nach der Aufnahme in einen Block die Differenz wieder gutgeschrieben.

Zur Veranschaulichung ist in Abbildung 27 eine beliebig ausgewählte Transaktion dargestellt (auf etherscan.io kann jeder validierte Block und die enthaltenen Transaktionen eingesehen werden).

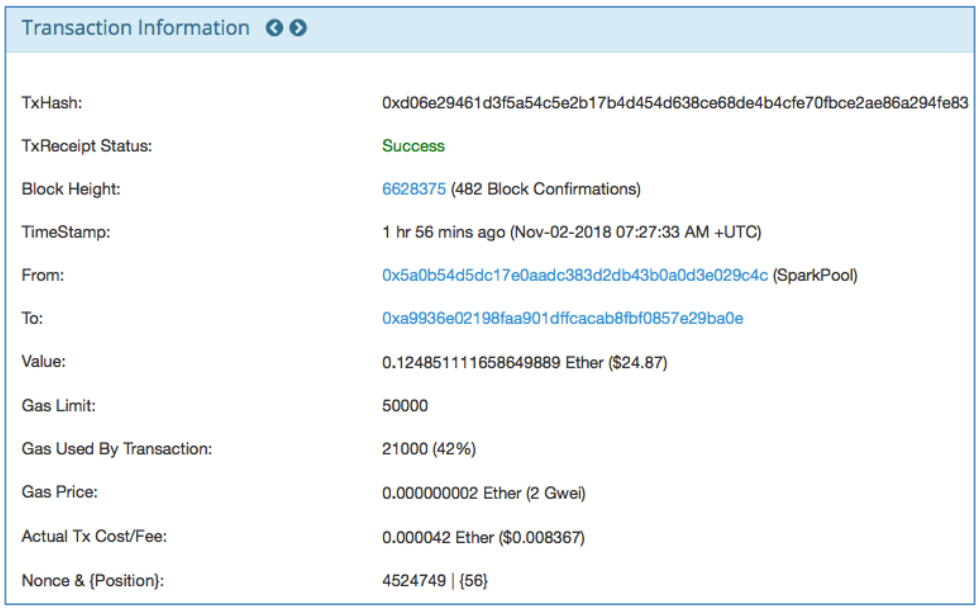

Abb. 27: Transaktion in Ethereum, Quelle (etherscan.io)

Der Initiator hat das Gas Limit auf 50.000 und den Gas Price auf 2 Gwei[10] festgelegt. Das ergibt Transaktionsgebühren von 50.000 Gas x 0,000000002 ETH = 0,0001 ETH, die er zu Beginn zu zahlen hat.

Das Ausführen der Transaktion hat tatsächlich nur 21.000 Gas verbraucht also

21.000 Gas x 0,000000002 ETH = 0,000042 ETH. Die Differenz von 0,000058 ETH wird ihm wieder gutgeschrieben.

Umfangreiche Smart Contracts erfordern mehr Rechenleistung, die geforderte Rechenleistung muss mit Gas vergütet werden. Umso komplizierter ein Vertrag programmiert wurde, desto mehr Rechenleistung wird benötigt und dementsprechend mehr Gas ist erforderlich, eine Transaktion auszuführen. Dieser Mechanismus soll neben dem Schutz des Netzwerks vor DoS[11] Angriffen, Entwickler dazu animieren, möglichst effiziente Smart Contracts zu programmieren. Gleichzeitig ist es aber sehr wichtig, beim Erstellen eines Smart Contracts ein korrektes Gas Limit und einen sinnvollen Gas Price festzulegen wie das folgende Beispiel in Abbildung 28 verdeutlicht.

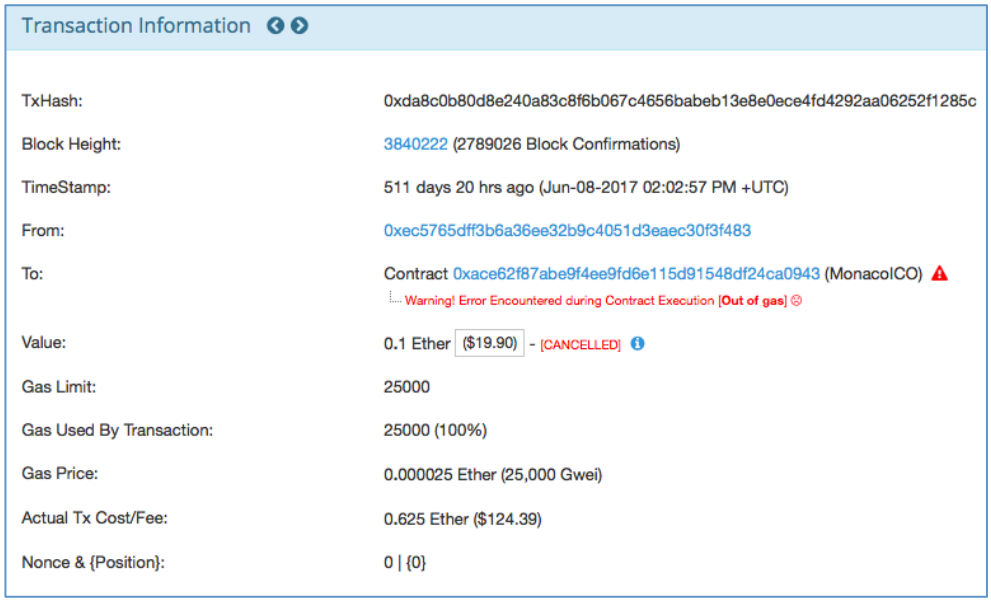

Abb. 28: Out of gas transaction, Quelle (etherscan.io)

Hier wurde das Gas Limit auf 25.000 gesetzt und der Gas Price auf 25 Gwei. Dies ergibt Transaktionsgebühren in Höhe von 25.000 Gas x 0,000025 ETH = 0,625 ETH. Das entsprach zu diesem Zeitpunkt einem Wert von 124,39 US$. Die 25.000 Gas haben aber nicht ausgereicht, um die durch den im Smart Contract enthaltenen Code notwendige Rechenleistung abzurufen, folglich lief die Transaktion „out of gas" und wurde nicht durchgeführt. Da die Transaktion trotzdem valide ist, erhält der Miner die vollen Transaktionsgebühren. Hier wurden gleich zwei folgenschwere Fehler gemacht. Erstens wurde das Gas Limit zu niedrig angesetzt, sodass die Transaktion nicht ausführbar wurde, und zweitens wurde der Gas Price viel zu hoch gewählt. Der Sender beabsichtigte 0,1 ETH = 19,90 US$ zu transferieren, und durch den gewählten Gas Price von 25 Gwei ergaben sich Transaktionsgebühren in Höhe von 0,625 ETH = 124,39 US$. Die Transaktionsgebühren stehen also in keinem Verhältnis zu dem zu transferierenden Betrag.

An dieser Stelle ist es wichtig zu verstehen, dass diese Form der Transaktionsabrechnung für die Ethereum Blockchain Gültigkeit besitzt. Innerhalb privater Blockchains, also Blockchains, die eine Zugangsberechtigung erfordern, kann auf die Erhebung von Transaktionsgebühren jedweder Form verzichtet werden. Unternehmen werden

[10] Gwei ist die kleinste Einheit in Ether; 1 ETH = 1.000.000.000 Gwei

[11] DoS - Denial of Service können unter anderem Netzwerke angreifen indem große Mengen an Anfragen, im Fall einer Blockchain eine große Menge an Transaktionen, das Netzwerk überlasten und reguläre Transaktionen behindern ("Denial of Service," 2018).

in den meisten Fällen in einem Blockchain Wertschöpfungsnetzwerk agieren, in dem durch die Vergabe von Zugangsberechtigungen alle Teilnehmer bekannt und identifizierbar sind. Angriffe durch übermäßig angestoßene Smart Contracts wären sinnlos und die Verursacher würden sofort identifiziert werden. Zudem stellt gerade die Reduzierung oder der Wegfall von Transaktionsgebühren einen ausschlaggebenden Vorteil der Blockchain Technologie dar. Das Gas Prinzip kann dennoch sinnvoll sein, um die maximal benötigte Rechenleistung von Smart Contracts zu begrenzen und um eine Überlastung durch fehlerhaft programmierte Verträge zu verhindern. Fehler im Programmcode können bspw. einen Infinity Loop (Endlosschleife) auslösen, welche die Berechnung einer Transaktion unendlich wiederholt und dadurch Rechenleistung belegt. Das Limitieren der verfügbaren Rechenleistung, durch das Setzen eines maximal verbrauchbaren Wertes wie Gas, verhindert das, indem nach Erreichen des Limits die Berechnung abgebrochen wird.

3.1.1 Smart Contract Code

Ethereum hat zum Erstellen von Smart Contracts die Programmiersprache Solidity[12] entwickelt. Das Hyperledger Projekt geht noch einen Schritt weiter und lässt auf ihrer Blockchain die Programmiersprachen Go, node.js und Java zu, sodass die Möglichkeiten für Entwickler von Smart Contracts und DApps noch vielfältiger sind. Smart Contracts werden im Hyperledger Projekt als Chaincode bezeichnet. In der Ethereum Blockchain werden Smart Contracts in Solidity geschrieben. Bedingungen und Regeln werden in dieser höheren Programmiersprache formalisiert. Um auf der EVM (Ethereum Virtual Machine, siehe 2.4.1) ausführbar zu werden muss der Code in einen maschinenlesbaren Bytecode kompiliert (übersetzt) werden. Damit der Smart Contract andere Verträge und Funktionen aufrufen kann muss ein Binärschnittstelle[13] (ABI - application binary interface) integriert sein (Dhillon et al., 2017, p. 36). Anhand eines einfachen Beispiels eines Crowdsale Contracts soll das IF→THEN Prinzip verdeutlicht werden.

SOLIDITY VERTRAGSQUELLCODE

```
44    /* checks if the goal or time limit has been reached and ends
45  function checkGoalReached() afterDeadline {
46      if (amountRaised >= fundingGoal){
47          fundingGoalReached = true;
48          GoalReached(beneficiary, amountRaised);
49      }
50      crowdsaleClosed = true;
51  }
52  function safeWithdrawal() afterDeadline {
53      if (!fundingGoalReached) {
54          uint amount = balanceOf[msg.sender];
55          balanceOf[msg.sender] = 0;
56          if (amount > 0) {
57              if (msg.sender.send(amount)) {
58                  FundTransfer(msg.sender, amount, false);
59              } else {
60                  balanceOf[msg.sender] = amount;
```

In einem Crowdsale Contract wird das Finanzierungsziel (funding goal) festgelegt. Ist das Ziel erreicht, soll der Crowdsale geschlossen werden. Im Code wird das formalisiert durch den markierten Bereich.

→If amount raised >= funding goal

→Then funding goal reached = true

→Then crowdsale closed = true.

Abb. 29: Bsp. Crowdsale Contract Code, erstellt mit Ethereum Wallet

Diese objektorientierte Programmiersprache vereinfacht es Entwicklern, Programmcode in einer logisch verständlichen Sprache zu erstellen. Dieser Code wird dann mittels eines Compilers in einen maschinenlesbaren Bytecode übersetzt.

[12] Solidity ist eine objektorientierte, anwendungsspezifische höhere Programmiersprache mit einer JavaScript-ähnlichen Syntax zum Entwickeln von Smart Contracts für die Ethereum-Blockchain-Plattform (GitHub, 2018).

[13] ABI – definiert, wie der Programmcode auf Ebene der Maschinensprache auszusehen hat und erlaubt den Betrieb auf allen Systemen, die eine binärkompatible Schnittstelle zur Verfügung stellen, ohne dass neu kompiliert werden muss ("Binärschnittstelle," 2018).

3.1.2 Oracles / Chain Link

Oracles, auch Chain Links genannt, sind ein wichtiger Bestandteil des Smart Contract Konzeptes. Smart Contracts können nicht auf externe Daten zugreifen, die zur Ausführung notwendig sein könnten. In einem Wertschöpfungsnetzwerk könnten das bspw. Informationen zu Lagerbeständen, Rohstoffpreisen oder Daten von Maschinen aus der Fertigung sein. Oracles können verwendet werden, um solche externen Daten Smart Contracts bereitzustellen. Ein Oracle ist eine Schnittstelle, die Daten von einer externen Quelle an Smart Contracts liefert. Oracles sind in der Lage, Daten digital zu signieren um den Nachweis zu erbringen, dass die Quelle der Daten authentisch ist. Smart Contracts können dann die Oracles abonnieren, sodass Smart Contracts entweder die Daten abrufen können oder das Oracle die Daten weiterleitet. Oracles dürfen dabei nicht in der Lage sein, die Daten zu manipulieren und dürfen nur authentische Daten bereitstellen. Um die Authentizität der von den Oracles aus externen Quellen bezogenen Daten nachzuweisen, können Mechanismen verwendet werden, die den Kommunikationsnachweis zwischen der Datenquelle und dem Oracle erbringen. Dadurch wird sichergestellt, dass die an den Smart Contract zurückgegebenen Daten definitiv aus der angegebenen Quelle stammen (Bashir, 2017).

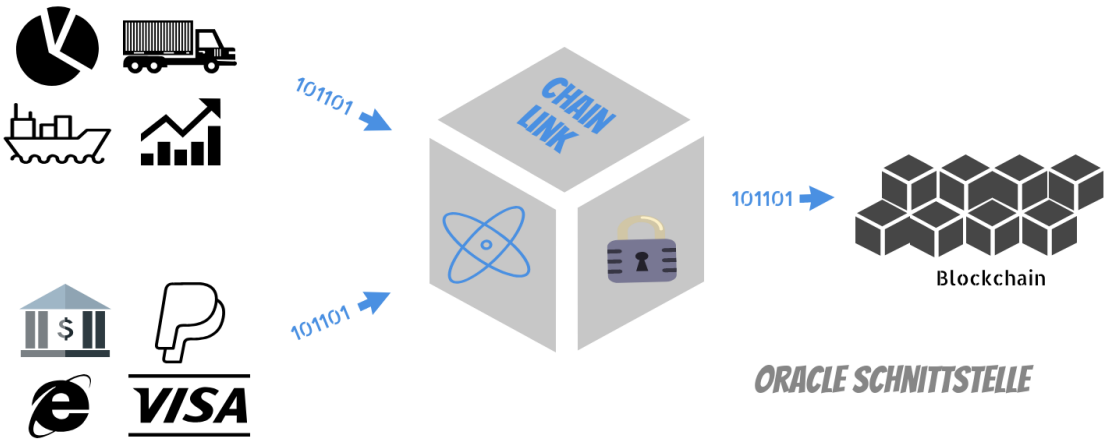

Abb. 30: Oracle Schnittstelle, eig. Darstellung vgl. (smartcontract.com, 2018)

Wenn Oracles auf zentral organisierte Datenbanken zugreifen, stellt sich natürlich wieder die Vertrauensfrage. Diese Art der Datenquelle erfordert das Vertrauen in eine dritte Instanz, die durch die zentralisierte Datenspeicherung und Verwaltung die Datenhoheit besitzt. Die Lösung bietet auch hier wieder ein dezentral organisiertes System. Ein Oracle kann auf der Grundlage eines verteilten Mechanismus aufgebaut werden. Das Oracle bezieht dabei die Daten aus anderen Blockchains , die durch dezentrale Konsensbildung gesteuert werden und so die Authentizität der Daten gewährleistet. So kann beispielsweise ein Unternehmen, das seine eigene private Blockchain betreibt, Daten über ein Oracle zur Verfügung stellen, die dann von Smart Contracts auf anderen Blockchains genutzt werden können. In cyber-physischen Systemen kommunizieren Maschinen und Objekte direkt miteinander. Um Smart Contracts effektiv einzusetzen ist es erforderlich, dass Objekte eines cyber-physischen System Informationen in Echtzeit über ein Oracle an Smart Contracts senden. Dabei muss sichergestellt werden, dass die Objekte gegen unerwünschte Manipulation gesichert werden. In privaten Blockchains kann es auch sinnvoll sein, auf herkömmlich, zentral organisierte Datenbanken zurückzugreifen. Dazu müssen sich allerdings alle Parteien des Netzwerkes vertrauen.

3.2 Anwendungsbeispiel Smart Contract

Smart Contracts ermöglichen die Automatisierung von Prozessen und Regularien. Anhand eines Beispiels wird eine mögliche Anwendung beschrieben und dargestellt, wie ein Smart Contract in einem Workflow implementiert sein kann. Beispiel: Ein Unternehmen möchte eine Spedition beauftragen, eine Maschine von A nach B zu transportieren. Abbildung 31 stellt den Ablauf grafisch dar, die Prozessschritte werden im Anschluss beschrieben.

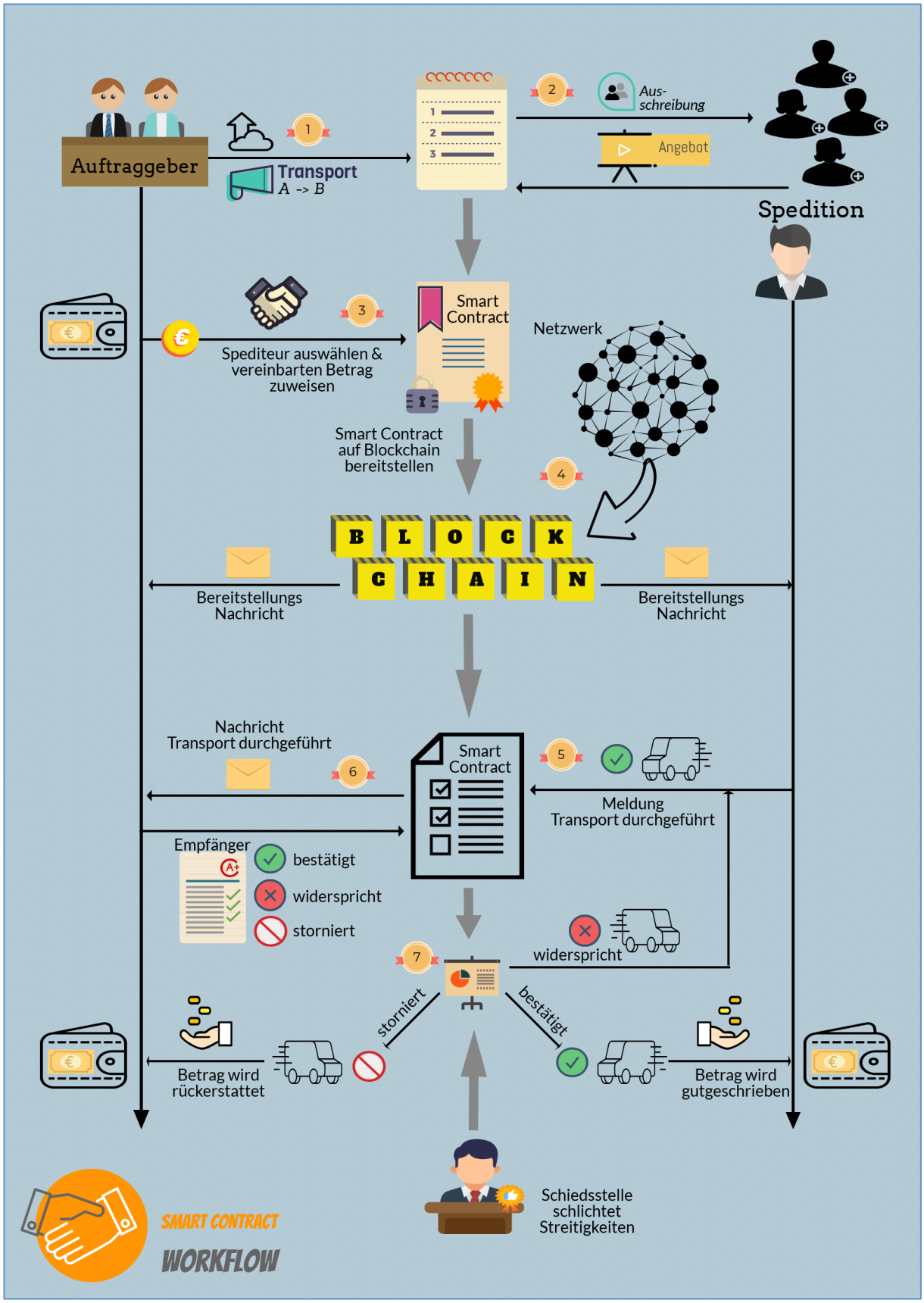

Abb. 31: Beispiel Smart Contract Workflow, eig. Darstellung angelehnt an (Patel et al., 2018, p. 157)

1. Der Auftraggeber definiert die Bedingungen des Transportes und formalisiert sie in einem Smart Contract.
    - Transportgut, in dem Beispiel eine Maschine, mit Angaben zu Gewicht, Abmessungen sowie notwendige Angaben zu Stoffen und Materialien soweit gesetzlich vorgeschrieben.
    - Abholadresse und Zieladresse.
    - Zeitangaben für Abholung und Ablieferung.
    - Sonstige Bedingungen und geforderte Leistungen.
    - Stornierungsbedingungen.
2. Der Smart Contract wird zur Ausschreibung online veröffentlicht. Speditionen oder sonstige potenzielle Auftragnehmer können Angebote erstellen und dem Auftraggeber vorlegen.
3. Der Auftraggeber entscheidet sich für ein Angebot und übernimmt die Angaben zu Preis und sonstigen Bedingungen des Auftragnehmers in den Smart Contract. Zudem muss er den Betrag des vereinbarten Preises an den Smart Contract allokieren. In dargestellten Beispiel wurde die Währung € gewählt, steht hier aber stellvertretend für Kryptowährung.
4. Der Smart Contract wird auf der Blockchain bereitgestellt. Das Netzwerk prüft, ob alle Bedingungen erfüllt sind. Also in diesem Fall, ob die Sender- und Empfängeradresse korrekt und bekannt sind. Gleichzeitig wird validiert, dass der Kontostand des Senders ausreichend gedeckt ist. Ist alles korrekt, wird der Smart Contract in einen Block aufgenommen und ist Teil der Blockchain. Er ist nun also auf jedem am Netzwerk beteiligten Node aktiv.
5. Sobald der Transport durchgeführt wurde erhält der Smart Contract eine Nachricht, dass diese Bedingung erfüllt wurde. Dies kann manuell durch den Spediteur über ein API (Application Programming Interface) eingegeben werden. Natürlich gibt es hier verschiedene Möglichkeiten und hängt davon ab, inwieweit das entsprechende Netzwerk bereits die Transformation zu einem cyber-physischen System vollzogen hat. In einem vollständig vernetzten System würde diese Nachricht automatisch ausgelöst werden, bspw. durch den Wareneingangs-Scan des Empfängers. Durch diesen Input ändert sich der Zustand, also der State Root des Smart Contracts, und muss somit wieder durch das Netzwerk validiert werden.
6. Durch die Änderung des Zustandes löst der Smart Contract eine Nachricht an den Auftraggeber aus. Dieser prüft, ob der Transport entsprechend den Vertragsbedingungen ausgeführt wurde. Dem Beispiel folgend meldet der Auftraggeber ebenfalls manuell über ein API an den Smart Contract zurück (auch hier ist eine automatisierte Rückmeldung denkbar; Eingangsscan, fehlender Scan, usw.). In diesem Beispiel hat er drei Optionen zur Rückmeldung:
    - Bestätigung: Er bestätigt die vertragsgemäße Durchführung des Transportes.
    - Widerspruch: Er widerspricht der vertragsgemäßen Durchführung. Das könnte bspw. eine verspätete Anlieferung beim Empfänger sein, oder dass die Maschine noch gar nicht angeliefert wurde.
    - Stornierung: Falls der Auftraggeber es für notwendig hält, den Transportauftrag neu zu vergeben. Bspw. wenn der Spediteur nicht mehr in der Lage sein sollte, den Auftrag auszuführen. Stornierungsbedingungen müssen im Smart Contract definiert sein.
7. Entsprechend dem Input führt der Smart Contract die entsprechende Transaktion aus:
    - Bestätigung: Auftrag wird abgeschlossen und der vereinbarte Betrag dem Konto des Auftragnehmers gutgeschrieben.
    - Widerspruch: Der Auftragnehmer erhält die Möglichkeit zur Nacherfüllung. In diesem Beispiel kann er bei einer Nicht-Lieferung die Auslieferung nachholen.
    - Stornierung: Kann der Auftrag vertragsgemäß storniert werden, wird der Auftrag storniert, und dem Auftragnehmer wird der im Smart Contract hinterlegte Betrag rückerstattet.

- Im Streitfall wird eine Schiedsstelle notwendig, da Smart Contracts lediglich anhand der im Code formalisierten Bedingungen Aktionen ausführen können. Es ist also unbedingt notwendig, möglichst genau Vertragsbedingungen zu definieren und im Smart Contract zu formalisieren.

Das Beispiel zeigt, wie ein Smart Contract in einen Workflow intergiert werden kann, bei dem bisher viele Prozesse manuell ausgelöst werden müssen. Auftragsbedingungen und Konditionen können konkret in Smart Contracts abgebildet werden. Fragen der Haftung und juristische Unstimmigkeiten müssen im Streitfall allerdings weiterhin von anderer Stelle geklärt werden. Ausschreibung und Angebot werden auch heute schon ohne Smart Contracts online über entsprechende Plattformen ausgetauscht. Neu ist, dass durch Smart Contracts schon alle Aktionen durch die IF→THEN→ELSE Beziehungen im Code klar definiert sind und automatisiert bei Eintreffen des entsprechenden Ereignisses ausgeführt werden. Durch die Blockchain ist es nicht möglich, Vertragsbedingungen nachträglich zu ändern oder zu manipulieren. Deshalb ist es entscheidend, dass beim Erstellen eines Smart Contracts keine Fehler oder falsche Angaben programmiert werden. Das ist definitiv die Schwachstelle des Konzeptes, da alle Parteien eines Smart Contracts in der Lage sein müssen, den Code zu lesen und vollständig zu verstehen. Einmal aktivierte Smart Contracts können nicht ohne weiteres gestoppt werden. Um Fehler zu korrigieren muss ein neuer Smart Contract aufgesetzt werden mit entsprechenden Korrekturaktionen. Es ist daher notwendig, dass in Zukunft jeder Geschäftsanwender Smart Contracts über eine grafische Benutzeroberfläche oder durch eine textbasierte Spracheingabe konfigurieren kann.

Überträgt man dieses einfache Beispiel eines einzigen Smart Contracts auf ein Wertschöpfungsnetzwerk, in dem mehrere Partner global kooperieren, deutet sich das Potenzial des Konzeptes an, Transaktionskosten und Gebühren für Banken und sonstigen vermittelnden Stellen einzusparen. In cyber-physischen Systemen ist es vorstellbar, dass Maschinen und Transporteinheiten über Smart Contracts Aktionen ausführen und direkt abrechnen.

3.3 Decentralized Applications

Dezentrale Anwendungen (DApps) sind Anwendungen, die auf einem P2P-Netzwerk von Computern ausgeführt werden. DApps gibt es schon seit der Einführung von P2P-Netzwerken. Es handelt sich um eine Art von Softwareprogramm, das so konzipiert ist, dass es im Internet nicht von einer einzigen Plattform kontrolliert wird. Dezentrale Anwendungen müssen nicht unbedingt auf einem Blockchain-Netzwerk laufen. BitTorrent, Napster, Tor sind alles traditionelle DApps, die über ein P2P-Netzwerk laufen, aber nicht auf einer Blockchain (Voshmgir and Kalinov, 2017, p. 30).

- **Traditionelle Webanwendung** verwendet HTML, CSS und Javascript, um eine Seite darzustellen. Zur vollständigen Anzeige müssen Daten aus einer Datenbank abgerufen werden, die ein API (Application Programming Interface) verwendet. Wenn man sich auf Facebook anmelden will, ruft die Seite ein API auf, um die persönlichen Daten zu erfassen und auf der Seite anzuzeigen.

  Traditionelle Websites: Front End → API → Datenbank

- **DApps** sind vergleichbar mit einer herkömmlichen Webanwendung. Das Frontend verwendet genau die gleiche Technologie, um die Seite darzustellen. Der einzige entscheidende Unterschied besteht darin, dass anstelle einer API-Verbindung zu einer Datenbank ein Smart Contract mit einer Blockchain verbunden ist.

  DApp-fähige Website: Front End → Smart Contract → Blockchain

Im Gegensatz zu traditionellen, zentralisierten Anwendungen, bei denen der Backend-Code auf zentralen Servern läuft, lassen DApps ihren Backend-Code auf den Nodes eines dezentralen P2P-Netzwerk (Blockchain) laufen. Dezentrale Anwendungen bestehen aus dem gesamten Paket, vom Backend bis zum Frontend. Smart Contracts bestehen aus dem Backend und oft nur aus einem kleinen Teil der gesamten DApp. DApps bestehen aus einer

Kombination mehrerer Smart Contracts und benötigen zusätzlich ein Front End für die Anwender (Voshmgir and Kalinov, 2017, p. 30).

3.4 Key Facts Smart Contracts

Die Fakten zu dem Konzept der Smart Contracts zusammengefasst, vgl. dazu (Mougayar and Buterin, 2016):

- Smart Contracts sind nicht dasselbe wie eine vertragliche Vereinbarung. Ein Smart Contract kann eine funktionale Anforderung durchführen und den Nachweis erbringen, dass bestimmte Bedingungen erfüllt oder nicht erfüllt wurden.
- Smart Contracts sind kein Gesetz. Sie sind als Computerprogramme die Basistechnologie, aber die Konsequenz ihrer Handlungen könnte Teil einer rechtsgültigen Vereinbarung sein. Fragen zur Rechtsfähigkeit und Maschinen als juristische Personen im Sinne des Gesetzes zu betrachten sind weiterhin ungeklärt.
- Smart Contracts beinhalten keine künstliche Intelligenz. Smart Contracts sind Programmcodes, die eine Geschäftslogik abbilden und auf einer Blockchain ausführen. Sie werden durch externen Input ausgelöst und können dadurch andere Smart Contracts oder Aktionen auslösen. Man kann sie als ein ereignisgesteuertes Konstrukt betrachten.
- Smart Contracts sind nicht dasselbe wie DApps. Smart Contracts sind in Kombination Teil einer DApp, und in der Regel existieren mehrere Smart Contracts innerhalb einer DApp.
- Smart Contracts sind relativ einfach zu programmieren. Komplexe Prozesse können in wenigen Zeilen Code durch einfache objektorientierte Programmiersprachen wie bspw. Solidity formalisiert werden. Es gibt fortgeschrittenere Implementierungen von Smart Contracts, die Oracles verwenden. Oracles sind Datenquellen, die verwertbare Informationen an Smart Contracts senden.
- Smart Contracts sind nicht nur für Entwickler gedacht. Es soll zukünftig möglich sein, intelligente Verträge über eine grafische Benutzeroberfläche oder eine textbasierte Spracheingabe zu erstellen.
- Smart Contracts sind sicher, wenn sie korrekt programmiert wurden. Die Schwachstelle ist das Programmieren. Einmal aktivierte Smart Contracts auf einer Blockchain sind gegen Manipulation durch das Netzwerk geschützt.
- Smart Contracts haben ein breites Anwendungsspektrum. In Wertschöpfungsnetzwerken und cyberphysischen Systemen bietet das Konzept zahlreiche Möglichkeiten in Verbindung zu Industrie 4.0.

Mougayar und Buterin haben in ihrem Buch „The Business Blockchain" Smart Contracts treffend in Kontext zur Blockchain formuliert:

> *„If trust ist he atomic unit of blockchains, then smart contracts are what programs the variety of trust unto specific applications."(Mougayar and Buterin, 2016)*

4. Anwendung im Supply Chain Management

Supply Chains werden durch die zunehmende globale Vernetzung immer komplexer, und die Transformation zu Industrie 4.0 stellt an das Supply Chain Management neue Anforderungen. Die Steuerung von Lieferanten, Produktion, Logistik und dem Versand innerhalb eines Supply Chain Network sind wichtiger Bestandteil von Industrie 4.0. Effiziente Supply Chains tragen entscheidend zur Wettbewerbsfähigkeit eines Unternehmens bei. Die Risiken für globale Supply Chains werden durch externe und interne Faktoren erhöht. Einige von ihnen sind Makrotrends, wie die Globalisierung und die globale Vernetzung, welche die Komplexität der Lieferketten erhöhen. Andere resultieren aus dem fortlaufenden Streben nach Effizienz, um Betriebskosten zu senken. Eine schlanke Fertigung, Just-in-Time, verkürzte Produktlebenszyklen, Outsourcing und Lieferantenkonsolidierung sind nur einige der Ansätze, die sowohl signifikante Verbesserungen als auch erhebliche Herausforderungen für das SCM mit sich bringen. Finanzprozesse in einer Supply Chain sind auch heute noch weitestgehend vom Wertschöpfungsprozess entkoppelt und ineffizient. So werden immer noch über 60 Prozent der B2B Transaktionen, auf Papierrechnungen basierend, abgerechnet. Durch die Integration einer Blockchain und Smart Contracts in die Struktur eines Supply Chain Network, können Prozesse automatisiert und Netzwerkteilnehmer einfacher integriert werden (Prinz and T.Schulte, 2017, p. 25). Zudem schafft die dezentrale Struktur eines einheitlich geführten Ledgers als Single-Source-of-Truth Transparenz und Vertrauen.

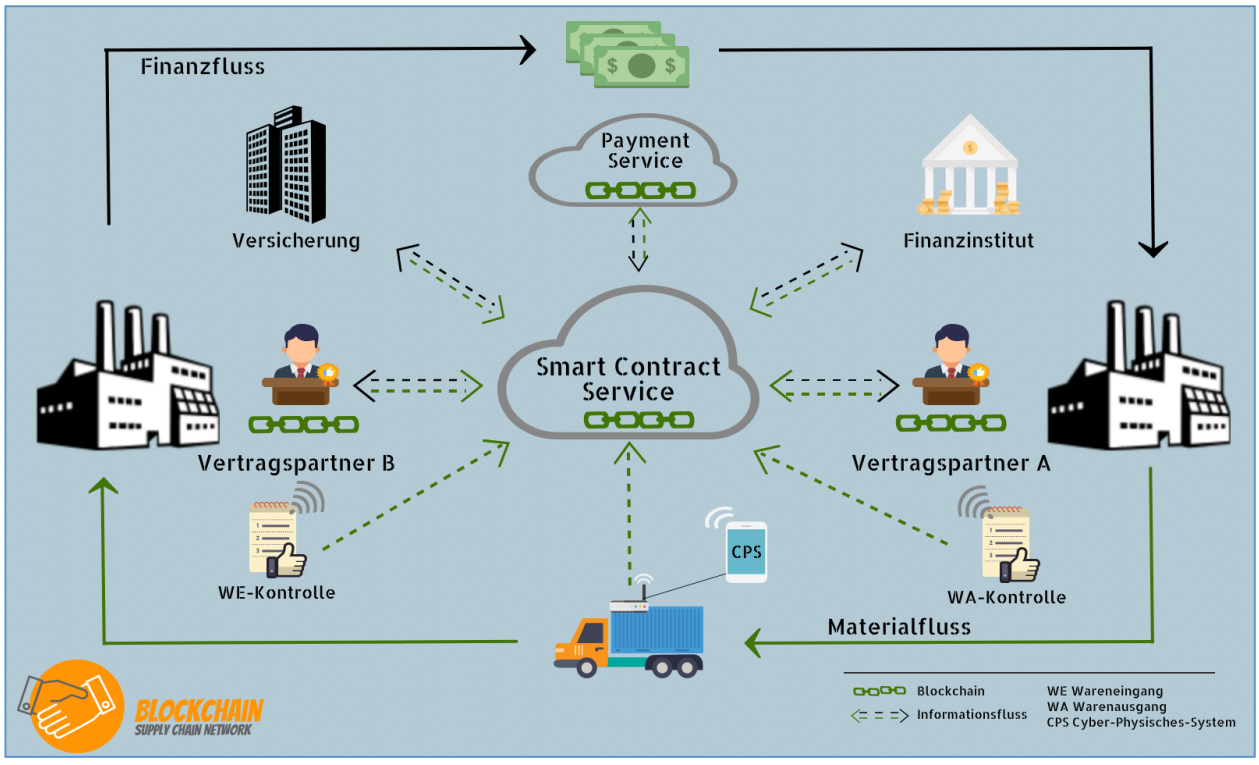

Abb. 32: Blockchain basiertes Supply Chain Network, eig. Darstellung vgl. (Prinz and T.Schulte, 2017, p. 25)

Die Fähigkeiten autonomer Dispositionsentscheidungen und automatisierter Transaktionsabwicklungen von Smart Contracts bieten enormes Potenzial zur Prozessoptimierung und Kostenreduzierung, gerade im Supply Chain Management (Prinz and T.Schulte, 2017, p. 25).

Bei der Implementierung einer Blockchain können zwei Ansätze verfolgt werden: innerhalb bestehender Organisationen, als Add-On-Technologie; oder von außerhalb einer Organisation, bspw. durch ein Startup, das möglicherweise nicht so sehr mit bestehenden Prozessen beschäftigt ist (Mougayar and Buterin, 2016).

Supply Chains und Supply Chain Networks haben jeweils sehr spezifische Ausprägungen und Eigenschaften, sodass es sinnvoll erscheint, aus der eigenen Organisation / dem eigenen Supply Chain Management die Implementierung einer Blockchain zu initiieren. Die Einbindung aller Netzwerkteilnehmer, also Lieferanten, Kunden, Speditionen usw., stellen dabei eine wesentliche Herausforderung dar. Zumal die meisten Unternehmen an mehreren Supply Chains und damit verschiedenen Wertschöpfungsnetzwerken beteiligt sind. Dabei stellt sich immer die Frage, welchen wirtschaftlichen Nutzen durch die Implementierung einer Blockchain gewonnen werden kann.

Um festzustellen, ob die Implementierung einer Blockchain und Smart Contracts in die Prozessstruktur einer Supply Chain tatsächlich das versprochene Potenzial zur Prozessoptimierung und Kostenreduzierung bietet, wird im Folgenden ein möglichst realistisches Szenario entwickelt. Dabei wird der Fokus auf die Prozesse der Auftragsabwicklung, der Beschaffung, der Kommissionierung und dem Versand gelegt, da das Konzept der Smart Contracts in diesen Bereichen ein hohes Potenzial zur Prozessoptimierung verspricht. Anhand einer Prozesskostenrechnung wird der wirtschaftliche Nutzen abgebildet. Eine abschließende Wirtschaftlichkeitsbetrachtung muss die notwendig werdende Investition rechtfertigen.

4.1 Supply Chain Szenario

Ein Maschinenbauer fertigt zwei Typen von Anlagen jeweils in einer Taktmontagelinie. Beide Typen können bis zu einem gewissen Grad vom Kunden individuell konfiguriert werden, bleiben aber trotzdem in beiden Linien montierbar. Nach der kundenspezifischen Konfiguration werden die Daten der Anlage der Disposition übergeben. Die Anlage wird im ERP-System disponiert, wodurch Bedarfsanforderungen generiert werden. Dabei wird geprüft, ob die Bedarfe an Kaufteilen durch Lagerbestände oder bestehende Bestellungen gedeckt sind. Ist das nicht der Fall, löst der Einkauf entsprechende Bestellungen bei den Lieferanten aus. Die Steuerung erstellt die entsprechenden Aufträge für das Logistikzentrum und die Montage. Zudem plant sie den zeitlichen Ablauf und beauftragt die Spedition für die Transporte vom Logistikzentrum zur Montage. Die Linien laufen im 2-Schichtbetrieb, fünf Tage die Woche. Eine Anlage wird in 5 Takten montiert, sodass von beiden Typen je 10 Anlagen in der Woche versandt werden. Eine Anlage besteht aus ca. 4.500 Einzelteilen, wobei ca. 1.000 Teile davon durch ein Kanban System direkt an den Montagelinien bereitgestellt werden. Die Kanbanversorgung wird durch einen Zulieferer sichergestellt. Die restlichen ca. 3.500 Einzelteile werden durch Zulieferer teilweise vormontiert geliefert, wodurch pro Anlage ca. 600 Bedarfe an Baugruppen und Einzelteilen im ERP-System generiert werden. Durch die weitgehende Standardisierung der beiden Anlagentypen können die Bedarfe zu Bestelllosgrößen zusammengefasst werden, sodass pro Anlage noch ca. 50 Einzelbestellungen notwendig sind. Das restliche Material wird über größere Bestellgrößen bestellt, sodass über einen längeren Zeitraum Bedarfe gedeckt werden. Das Lager und die Versorgung der Taktmontage wurde zu einem externen Logistikdienstleister ausgelagert. Dieser übernimmt die Vereinnahmung und Lagerung der gelieferten Baugruppen und Teile in seinem Logistikzentrum. Er übernimmt ebenfalls die Kommissionierung der Anlage und stellt alle Teile Just-in-time an den Montagelinien des Maschinenbauers bereit. Pro Anlage werden 2 Lkw zum Transport benötigt. Das gesamte Material einer Anlage wird zum Takt 1 bereitgestellt und während der 5 Takte verbaut. Das bedeutet; pro Schicht liefern vier Lkw zwei Anlagen an die beiden Montagelinien. An einem Tag müssen also vier Anlagen kommissioniert werden und acht Lkw-Transporte sind notwendig, um die Versorgung der Montage sicherzustellen. Nach der Montage werden die Anlagen verpackt und mit jeweils einem Lkw zum Kunden versendet. Die Abteilung Versand beauftragt die Spedition und verschickt die Rechnung an den Kunden. Abbildung 33 stellt den Ablauf grafisch dar.

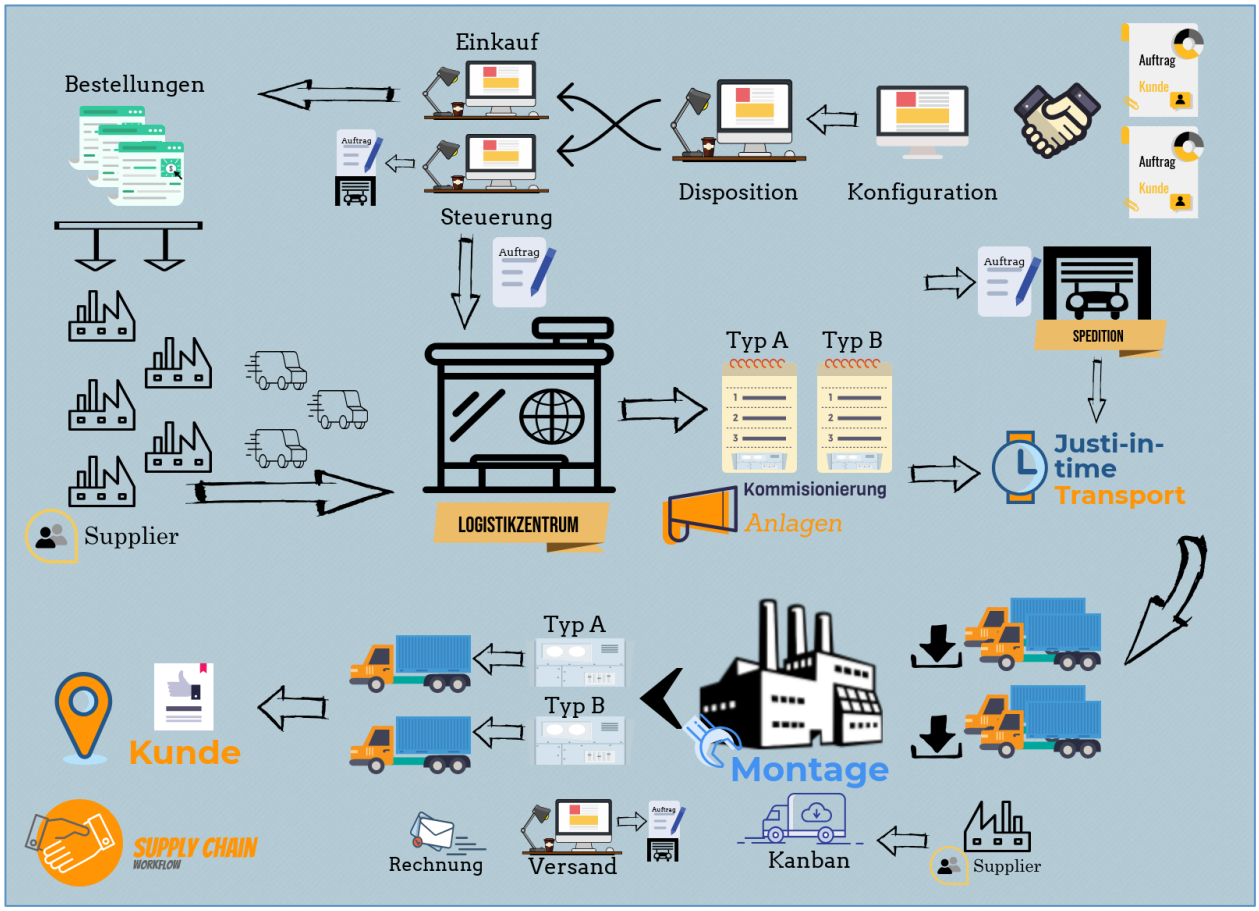

Abb. 33: SCM Workflow Maschinenbauer

Die Prozesse sind im Ablauf und Aufwand bei Typ A und Typ B identisch, lediglich die Montagelinien sind je Typ festgelegt. Die Prozesskosten des Maschinenbauers werden auf Monatsbasis ermittelt. Typ A und Typ B benötigen jeweils 5 Takte zum Montieren. Beide Montagelinien laufen im 2-Schichtbetrieb, 5 Tage die Woche. Dies ergibt je 10 Anlagen pro Woche Typ A und Typ B, im Monat 80 Anlagen gesamt. Die angesetzten Prozesszeiten und Stundensätze wurden von einem realen Beispiel entnommen und in ein Verhältnis gesetzt, um keine Rückschlüsse auf den Maschinenbauer zuzulassen.

4.1.1 Auftragsabwicklung

Die Auftragsabwicklung umfasst die Prozesse Konfiguration, Disposition und Auftragssteuerung.

- **Konfiguration:** Der Kunde hat die Möglichkeit, entsprechend seiner Anforderungen eine Anlage bis zu einem gewissen Grad zu konfigurieren. Ausgangspunkt ist immer die Standardanlage Typ A oder Typ B. Der Vertrieb klärt vor Auftragsvergabe die individuellen Kundenanforderungen und übergibt den Datencontainer der vom Kunden bestellten Anlage über das ERP-System an die Konstruktion. Ein Mitarbeiter konfiguriert anhand des Datencontainers die Anlage. Dazu müssen die Stückliste und der Montagearbeitsplan entsprechend angepasst werden. Die Anlage bleibt in jedem Fall in 5 Takten montierbar. Für die Konfiguration einer Anlage wird mit 3 Stunden gerechnet. Die konfigurierte Anlage wird dann an die Disposition übergeben.
- **Disposition:** Auf Grundlage des vereinbarten Liefertermins wird die Anlage im ERP-System disponiert. Jede Anlage erzeugt einen Bedarf an einem Fertigungsauftrag. Die Bedarfsermittlung gleicht die Bedarfe mit

vorhandenem Lagerbestand und bestehenden Bestellungen ab. Nicht gedeckte Bedarfe erzeugen Bestellanforderungen. Eine zeitliche und mengenmäßige Zusammenfassung der Bedarfe erfolgt anhand der Parameter Dispomerkmal, Losgröße, Mindest- und Maximallosgröße. Die Terminierung der Bestellanforderungen erfolgt anhand der Parameter Planlieferzeit, Bedarfsvorlaufzeit und Wareneingangs Bearbeitungszeit. Für das Disponieren einer Anlage wird mit 2 Stunden gerechnet.

- **Auftragssteuerung:** Anhand der erzeugten Bedarfe aus der Disposition erstellt die Auftragssteuerung die Aufträge zur Montage sowie zur Kommissionierung durch das Logistikzentrum und beauftragt die Spedition zum Transport der kommissionierten Anlage vom Logistikzentrum zum Montagewerk. Die Weiterleitung des Materials direkt an die Montagelinien erfolgt über die werksinterne Logistik. Die zeitliche Planung und Steuerung der Montagelinien erfolgt anhand der Liefertermine. Die Abstimmung zwischen Logistikzentrum, Spedition und Montage ist Teil der Steuerungsaufgaben.

Auftragsabwicklung	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Konfiguration	80	3 h	78 €	18.720 €
Disposition	80	2 h	76 €	12.160 €
Auftrag Montage	80	0,5 h	73 €	2.920 €
Auftrag Kommissionierung	80	0,5 h	73 €	2.920 €
Auftrag Transport	80	0,5 h	73 €	2.920 €
Prozesskosten Monat				**39.640 €**

Tab. 2: Prozesskosten Auftragsabwicklung

4.1.2 Beschaffung

Der Einkauf wählt Lieferanten aus, verhandelt Preise und Vertragsbedingungen. Zu den Bestellanforderungen werden Bestellungen im ERP-System ausgelöst, um die Bedarfe abzudecken. Pro Anlage wird mit 50 Einzel Bestellungen gerechnet, ergibt 4.000 Bestellungen pro Monat. Das restliche Material wird zu festgelegten Bestellgrößen zusammengefasst und deckt die Bedarfe über einen längeren Zeitraum ab. Es wird mit 1.000 weiteren auszulösenden Bestellungen im Monat gerechnet. Die Abrechnung der Kanbanversorgung erfolgt monatlich. Der Supplier schickt die Rechnung mit dem verbrauchten Material. Die Beschaffung prüft den Verbrauch und gibt die Rechnung zur Zahlung frei.

Beschaffung	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Bestellung auslösen	5.000	0,5 h	76 €	190.000 €
Kanban Abrechnung	1	2 h	76 €	152 €
Prozesskosten Monat				**190.152 €**

Tab. 3: Prozesskosten Beschaffung

4.1.3 Kommissionierung

Die Vereinnahmung und Lagerung sowie das Kommissionieren der Anlagen wurde zu einem Logistikdienstleister ausgelagert. Der Logistikdienstleister rechnet monatlich ab. Grundlage sind Anzahl Wareneingangsbuchungen und belegte m^2 im Lager. Dafür wurden je WE-Buchung 1,60€ und je belegtem m^2 7,20€ vereinbart. Die Kosten für die Kommissionierung einer Anlage werden ebenfalls monatlich, entsprechend der Anzahl kommissionierter Anlagen,

abgerechnet. Die abgerechneten Prozesskosten werden in die Prozesskostenrechnung des Maschinenbauers übernommen.

Kommissionierung	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Typ A kommissionieren	40	20 h	52 €	41.600 €
Typ B kommissionieren	40	20 h	52 €	41.600 €
WE Buchungen	ca. 7000		1,60 €/Buchung	11.200 €
Belegte qm^2	13.500 m^2		7,20 €/m^2	97.200 €
Prozesskosten Monat				**191.600 €**

Tab. 4: Prozesskosten Kommissionierung

4.1.4 Versand

Der Versand verpackt die Anlagen. Eine Spedition wird mit dem Transport zum Kunden beauftragt. Er erstellt die Rechnung und schickt sie an den Kunden. Betrachtet werden nur die administrativen Prozesskosten der Rechnungs- und Auftragserstellung.

Versand	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Auftrag Transport	80	0,5 h	69 €	2.760 €
Rechnung erstellen	80	0,25 h	69 €	1.380 €
Prozesskosten Monat				**4.140 €**

Tab. 5: Prozesskosten Versand

4.1.5 Kommunikation

Abbildung 34 stellt den Informationsfluss und die Transaktionsbeziehungen des Supply Chain Network dar. Der Maschinenbauer, das Logistikzentrum, die Supplier und die Speditionen führen jeweils ihr eigenes Ledger, indem Aufträge, Transaktionen und Eigentumsverhältnisse aufgezeichnet werden. Jedes Unternehmen operiert auf Grundlage seiner eigenen Datenbasis. Bestellungen und Aufträge werden in Papierform oder elektronisch übermittelt und müssen jeweils in das eigene System eingegeben werden. Änderungen müssen manuell abgestimmt und in beiden Systemen der Unternehmen übernommen werden. So existiert jeder Auftrag oder Bestellung auf mindestens zwei Systemen der jeweils beteiligten Unternehmen. Welchen Status eine Bestellung oder Auftrag hat, führt jedes Unternehmen lokal, sodass innerhalb des Supply Chain Network keine Transparenz über den Ausführungsgrad einer Bestellung oder eines Auftrages besteht. Es ist ein hoher Abstimmungsaufwand notwendig, um das zeitliche Zusammenspiel zwischen Supplier, dem Logistikzentrum, der Speditionen und der Montage sicherzustellen. Die Eigentumsverhältnisse von Komponenten und Anlagen werden ebenfalls in unternehmensinternen Ledger dokumentiert. So wissen die Supplier nicht, was mit den Komponenten passiert, nachdem sie im Logistikzentrum vereinnahmt wurden. Die Disposition des Maschinenbauers muss sich bei der Bedarfsermittlung auf die Lagerbestandsführung des Logistikzentrums verlassen, da keine einheitliche Datenbasis vorhanden ist. Die Spedition muss sich auf die Steuerung des Maschinenbauers verlassen, dass die zu transportierenden Anlagen zum vereinbarten Termin zur Abholung bereit stehen. Der Kunde weiß, ohne manuelle Abstimmung, nicht über den Fertigstellungsgrad seiner bestellten Anlage Bescheid. Er muss sich auf den vereinbarten Liefertermin verlassen. Abweichungen müssen manuell kommuniziert und abgestimmt werden.

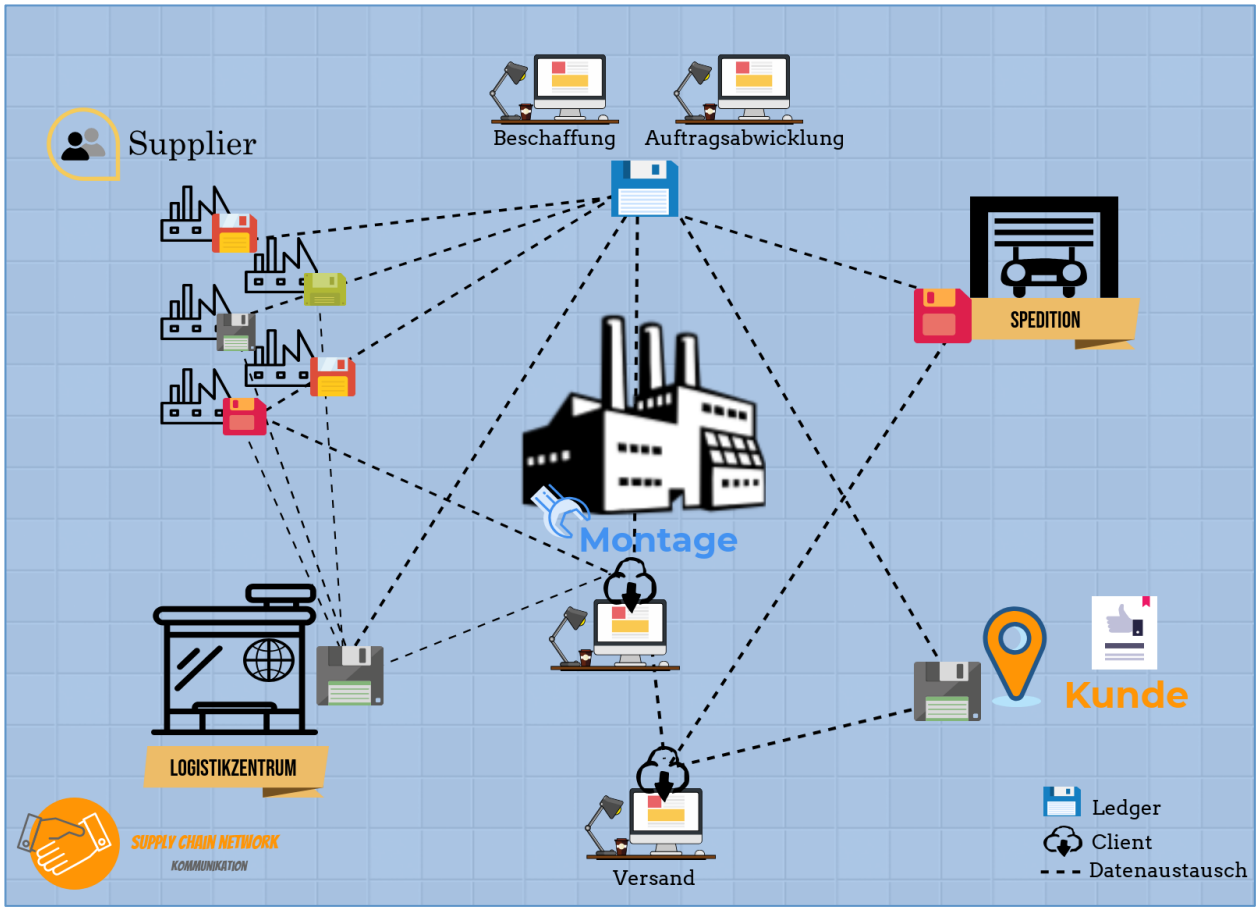

Abb. 34: Kommunikation im Supply Chain Network

Die Kommunikation innerhalb des Netzwerkes ist also ineffizient und mit hohem Aufwand verbunden.

Der Aufwand zur Abstimmung pro Anlage variiert je nach Kunde und Konfiguration. Der Abstimmungsaufwand ergibt sich aus der notwendigen Kommunikation zwischen dem Maschinenbauer, den Kunden, den Supplier, dem Logistikzentrum und der Spedition. Dabei geht es um die Planung und Steuerung der Aufträge und Bestellungen. Grundsätzliche Auftrags- und Lieferkonditionen werden dabei nicht betrachtet. Das Verhandeln der allgemeinen Einkaufs- und Lieferbedingungen, sowie Rahmen- und Speditionsverträge sind nicht Teil des in diesem Szenario betrachteten Prozesses und dementsprechend nicht Teil der Prozesskostenrechnung.

Prozesskosten des Abstimmungsaufwandes werden pauschal über einen Durchschnittswert pro Anlage berechnet.

Abstimmung	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Auftragsabwicklung	80	1 h	78 €	6.240 €
Beschaffung	80	1 h	76 €	6.080 €
Kommissionierung	80	0,5 h	73 €	2.920 €
Versand	80	0,5 h	73 €	2.920 €
Prozesskosten Monat				**18.160 €**

Tab. 6: Prozesskosten Abstimmung

Die Prozesskosten des Maschinenbauers eines Monats zusammengefasst:

Gesamt	Kosten pro Monat	Anlagen pro Monat	Kosten pro Anlage
Auftragsabwicklung	39.640 €	80	495,50 €
Beschaffung	190.152 €	80	2.376,90 €
Kommissionierung	191.600 €	80	2.395,00 €
Versand	4.140 €	80	51,75 €
Abstimmung	18.160 €	80	227,00 €
Prozesskosten Monat	**443.692 €**	**80**	**5.546,15 €**

Tab. 7: Prozesskosten Gesamt

Die Prozesskosten belaufen sich in Summe auf 443.692 € im Monat und 5.546,15 € pro Anlage. Es sei nochmal darauf hingewiesen, dass hier lediglich ein Teil der Prozesskosten betrachtet werden. Es wurden die Prozesse ausgewählt, bei denen in einem ersten Ansatz das größte Potenzial zur Optimierung durch die Integration einer Blockchain und Smart Contracts vermutet werden. Der Montageprozess wurde nicht betrachtet, dennoch könnten auch hier Synergieeffekte entstehen die zur Kostenreduzierung beitragen. Eine optimierte Supply Chain wirkt sich positiv auf die interne Werkslogistik und damit auch auf die Herstellkosten der Montage aus.

4.2 Integration einer Blockchain

Um in einem Supply Chain Network eine einheitliche Datenbasis zu schaffen, wäre in dem beschriebenen Szenario ein einheitliches ERP-System eine Lösung. Wenn alle beteiligten Unternehmen im selben System arbeiten würden, könnten Prozesse einfacher harmonisiert und der Abstimmungsaufwand deutlich reduziert werden. In einem relativ kleinen Supply Chain Network wäre dies umsetzbar, allerdings nur wenn die Teilnehmer ausschließlich in diesem Netzwerk agieren und dazu bereit sind, ihre Daten in einem gemeinsam genutzten ERP-System zu teilen. Dabei würden Fragen der Kostenverteilung und Verantwortlichkeiten der System-Administration zu beantworten sein. In der Regel sind Unternehmen an mehreren Supply Chains beteiligt, was diese Variante bereits ausschließt. Es muss also davon ausgegangen werden, dass Unternehmen weiterhin eigene ERP-Systeme unterhalten.

Die Integration einer Blockchain, und damit eines dezentral verteilten Ledgers, bietet einen Lösungsansatz, bei dem alle Netzwerkteilnehmer weiterhin in ihren ERP-Systemen arbeiten können. Ein gemeinsam genutztes Ledger, als Single-Source-of-Truth, bietet eine gemeinsame Datengrundlage und schafft dadurch Transparenz. Informationen zu Transaktionen, zu Lagerbeständen, zu Auftragsstatus und Lieferzeiten stehen in Echtzeit allen teilnehmenden Unternehmen zur Verfügung. Durch die gemeinsame Konsensbildung und die Unveränderlichkeit der in der Blockchain gespeicherten Daten wird Vertrauen innerhalb des Supply Chain Network geschaffen. Unternehmensinterne Daten obliegen weiterhin der Datenhoheit der beteiligten Unternehmen, da nur die für eine Transaktion notwendigen Informationen auf der Blockchain veröffentlicht werden müssen. Unternehmen sind in der Regel in mehreren Wertschöpfungsnetzwerken aktiv und können an mehreren Blockchains partizipieren.

In Abbildung 35 ist die Blockchain basierte Kommunikation dargestellt. Der Informationsaustausch findet über ein dezentral verteiltes Ledger statt. Dadurch entsteht eine gemeinsame Datenbasis, auf die beteiligte Unternehmen in Echtzeit Zugriff haben. Ineffizienzen der Kommunikation können so beseitigt werden und es entsteht Transparenz innerhalb des Supply Chain Network.

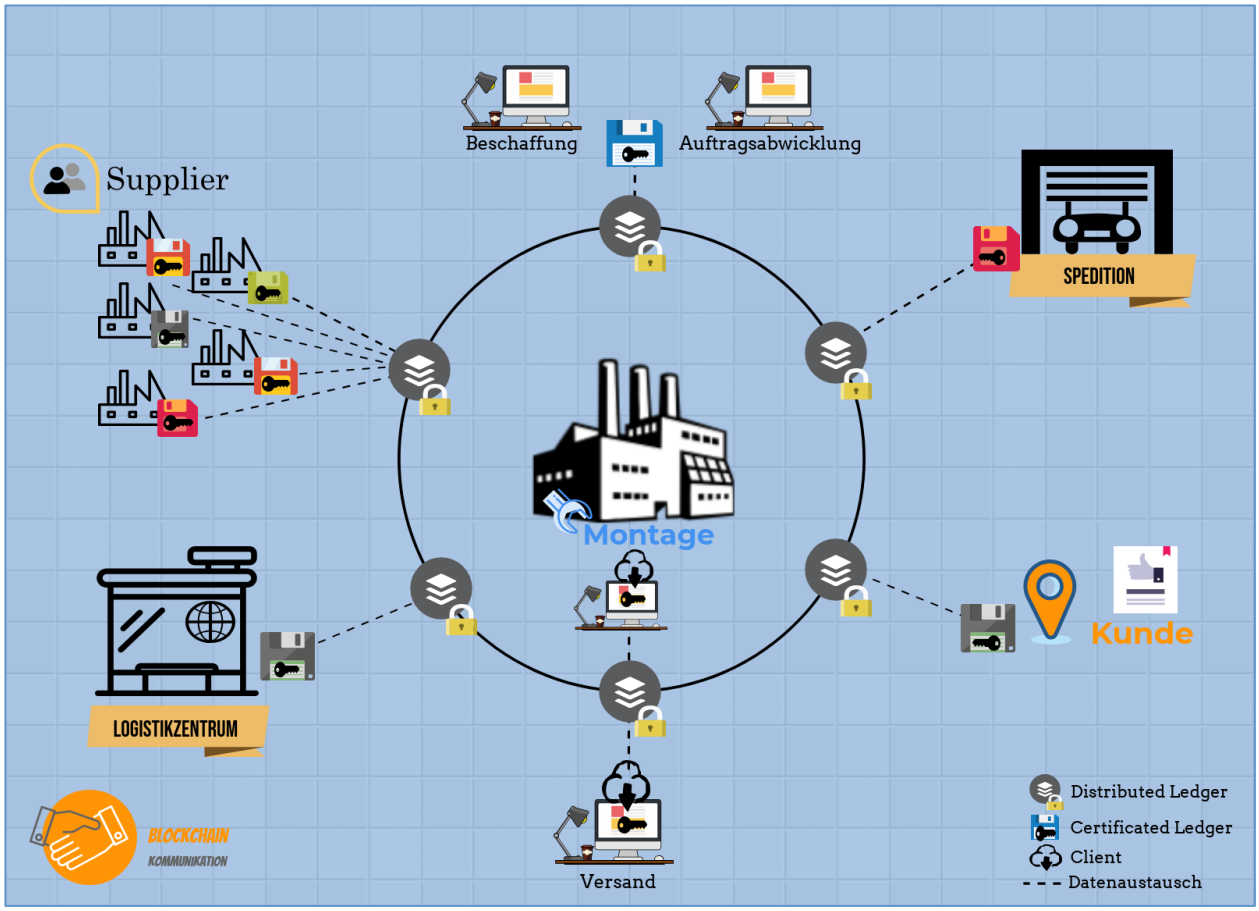

Abb. 35: Blockchain basierte Kommunikation

In einem Supply Chain Network ist es für Unternehmen notwendig, Daten und Informationen auszutauschen und die entstehende Transparenz durch die Integration einer Blockchain bringt wesentliche Vorteile. Allerdings wird es kaum ein Unternehmen geben, welches bereitgestellte Daten und Informationen der breiten Öffentlichkeit zugänglich machen möchte, da dies Angriffspunkte zum Datendiebstahl und Manipulationsversuchen bieten würde. In Frage kommen von daher nur private Blockchains, bei der alle Teilnehmer bekannt und identifizierbar sind. Über eine Zertifizierungsstelle werden Zugangsberechtigungen vergeben, nachdem sich die Unternehmen registriert haben. Dabei können Sicherheitsstufen definiert werden, die festlegen, wer Zugang zum Ledger erhält und auf welche Informationen Zugriff gewährt wird. So können auch untereinander konkurrierende Unternehmen des Supply Chain Network Daten einander unzugänglich machen. Konsens über die Vergabe von Zugangsberechtigungen innerhalb des Supply Chain Network kann durch den Konsensfindungsmechanismus der Blockchain erreicht werden. So wird sichergestellt, dass nur Unternehmen Zugang zum dezentral verteilten Ledger erhalten, die durch das Netzwerk dazu berechtigt wurden.

Das Proof of Work (PoW) Verfahren ist zur Konsensfindung in einem Netzwerk mit begrenzter Anzahl an Teilnehmern nicht sinnvoll. Beim PoW entscheidet die zur Verfügung gestellte Rechenleistung über das Recht Transaktionen zu einem Block zusammenzufassen und zu validieren. Der Miner, der die meiste Rechenleistung zur Verfügung stellt und dabei 51% der dem Netzwerk, durch alle Miner zur Verfügung gestellten Rechenleistung erreicht, könnte das Netzwerk beherrschen und wäre in der Lage Transaktionen und somit die Blockchain zu manipulieren. In einer privaten Blockchain, in der alle Teilnehmer bekannt sind, scheint es auch nicht sinnvoll zur Konsenserreichung Energie in Form von Rechenleistung zu verbrauchen. Auch die Kosten für die notwendige Hardware kann gespart werden.

Als Konsensfindungsmechanismus bietet sich das Proof of Authority (siehe 2.3.5.5) Verfahren an. Durch die begrenzte Anzahl an Netzwerkteilnehmern kann durch ein demokratisches Verfahren Konsens bei der Validierung von Transaktionen geschaffen werden. Die Netzwerkteilnehmer einigen sich auf Authority Nodes. Dabei bietet sich an, dass jedes beteiligte Unternehmen einen solchen Authority Node betreibt. Dadurch sind alle Unternehmen beim Validierungsprozess vertreten und im Besitz der gleichen Rechte. Dabei kann festgelegt werden, dass eine Mehrheit ausreicht um einen Block zu validieren, oder dass alle beteiligten Authority Nodes dem Validieren zustimmen müssen. Auf die Ausgabe von Tokens kann verzichtet werden. Dementsprechend ist es auch nicht notwendig, die Rechtevergabe zur Blockerstellung an den Tokenbestand eines Nodes zu knüpfen. Die Rechte zum Minen eines neuen Blocks werden rundenbasiert vergeben. Da für das Minen eines neuen Blocks keine Belohnung ausgegeben wird, spielt es für die Netzwerkteilnehmer keine Rolle, wer letztendlich einen neuen Block der Blockchain hinzufügt. Durch die rundenbasierte Vergabe der Validierungsrechte wird sichergestellt, dass jedes Unternehmen am Validierungsprozess beteiligt ist und dadurch Konsens geschaffen.

Nachdem eine bestimmte Anzahl an Transaktionen von einem Authority Node zu einem Block zusammengefasst und im Netzwerk veröffentlicht wurde, wird er durch die anderen Authority Nodes des Netzwerkes validiert. Dazu werden anhand des Merkle Roots und des Block Headers die enthaltenen Transaktionen geprüft. Nach erfolgreicher Prüfung wird der Block der lokal gespeicherten Blockchain angefügt und so im Netzwerk verbreitet. Alle anderen Nodes können zwar keine neuen Blöcke erstellen und auf der Blockchain speichern, sie sind aber trotzdem in der Lage, die Integrität der Blockchain anhand des Block Headers und des Merkle Roots zu validieren.

Aufgrund der relativ kleinen Anzahl an Netzwerkteilnehmern und der im Verhältnis geringen Anzahl an Transaktionen wird der Speicherbedarf der Blockchain relativ langsam wachsen. Dennoch kann es auch hier sinnvoll sein, nicht alle Nodes als Fullnode zu betreiben. Gerade auf Tablets, Notebooks oder sonstigen mobilen Geräten kann das SPV-Konzept (Simple Payment Verification) ausreichend sein. Bei diesem Verfahren wird lediglich der Block Header aller bisherigen Blöcke auf dem Gerät gespeichert und anhand des enthaltenen Hashwertes validiert (siehe 2.3.2 Fullnode vs. SPV, S.23).

Besondere Hardware Anforderungen bestehen sowohl an die Authority Nodes als auch an alle anderen Nodes nicht. Da bei PoA kein rechenintensives kryptografisches Rätsel zu lösen ist wie bei PoW, muss keine gesonderte Hardware angeschafft werden. Jeder gängige PC oder Laptop verfügt heutzutage über ausreichend CPU-Leistung und Speicher.

4.3 Integration von Smart Contracts

Die Integration einer Blockchain schafft also vor allem Transparenz und optimiert die Kommunikation durch Schaffung einer gemeinsamen Datengrundlage. Die Integration von Smart Contracts in die Prozesslandschaft des Supply Chain Network kann zudem Abläufe automatisieren und manuelle Prozesse zum Teil ersetzen. Wie in Kapitel 3 beschrieben sind Smart Contracts in Code übersetzte Regeln und Bedingungen. Sie sind in der Lage, Transaktionen selbständig auszuführen, wenn ein bestimmtes Ereignis eintritt oder eine definierte Bedingung erfüllt wird. In einem Supply Chain Network gibt es eine Vielzahl von Regeln, Vereinbarungen, Konditionen, Bedingungen, usw., die zwischen den beteiligten Unternehmen ausgehandelt werden. Bei der Integration von Smart Contracts in die Prozesse des Netzwerkes müssen zu jedem Prozess, die jeweils definierten Regeln und Bedingungen in Programmcode übersetzt werden. Eine objektorientierte Programmiersprache vereinfacht es, Programmcode in einer logisch verständlichen Sprache zu erstellen. Dennoch ist es notwendig, den Code eines Smart Contracts durch kompetente Programmierer zu erstellen. Da es einen viel zu hohen Aufwand darstellen würde, für jede neue Transaktion einen Smart Contract zu erstellen, bietet es sich an, zu allen Prozessen Vorlagen zu erstellen, bei denen dann nur noch einzelne Parameter, wie bspw. Empfänger, Liefertermine usw., eingefügt werden müssen. Da nicht davon ausgegangen werden kann, dass jeder Anwender in der Beschaffung, dem Versand usw., über ausreichend Programmierkenntnisse verfügt, ist es notwendig, ein Frontend bereitzustellen, über das Parameter einfach eingetragen werden können. Hier kommen die unter 3.3 beschriebenen DApps zur Anwendung, wobei Smart Contracts das Backend bilden. Zudem ermöglichen DApps als Software Anwendungen, die auf einem P2P-Netzwerk ausgeführt werden, die Interaktion der Netzwerk-

teilnehmer. Damit Smart Contracts auf Daten der ERP-Systeme zugreifen können, um bspw. Lagerbestände abrufen zu können, müssen die unter 3.1.2 beschriebenen Oracles als Schnittstelle integriert werden. Sie sind in der Lage Daten, digital zu signieren und Quellen zu authentifizieren.

4.3.1 Auftragsabwicklung

In der Auftragsabwicklung können Smart Contracts in den folgenden drei Bereichen verschiedene Aufgaben übernehmen:

- **Konfiguration:** Smart Contracts können die Konfiguration einer Anlage übernehmen. Dazu müssen die Daten der vom Kunden gewünschten Konfiguration über eine DApp im Code verankert werden. Der Smart Contract kann dann nach dem IF→THEN Prinzip die Konfiguration vornehmen und Stücklisten und Arbeitspläne anpassen. Abschließend wird der nachfolgende Smart Contract der Disposition ausgelöst. Die so automatisierte Konfiguration muss abschließend kontrolliert und freigegeben werden. Der Aufwand hierfür reduziert sich auf 0,5h.
- **Disposition:** Die Disposition einer Anlage kann vollständig automatisiert durch einen Smart Contract erfolgen. Ausgelöst durch den Konfigurations-Contract kann er anhand der übermittelten Stücklisten und Arbeitspläne Bedarfe erzeugen und über das entsprechende Oracle mit Lagerbeständen und vorhandenen Bestellungen abgleichen. Nicht gedeckte Bedarfe erzeugen Bestellanforderungen. Die Terminierung der Bestellanforderungen erfolgt anhand der im Code hinterlegten Parameter Planlieferzeit, Bedarfsvorlaufzeit und Wareneingangs-Bearbeitungszeit.
- **Auftragssteuerung:** Aufträge zur Montage, zur Kommissionierung und für die Spedition werden durch den Dispositions-Contract ausgelöst. Anhand der im Code hinterlegten Bedingungen und Konditionen werden die Aufträge in Form von Smart Contracts erstellt und auf der Blockchain veröffentlicht. Beim Abschließen der Aufträge werden Bedingungen des Smart Contract erfüllt und der entsprechende Abrechnungsprozess kann ebenfalls über einen Smart Contract abgewickelt werden.

Die weitgehende Automatisierung der Prozesse bedeutet für die Mitarbeiter eine grundlegende Änderung ihres Aufgabengebietes. Das Aufgabenfeld wandelt sich von der Sachbearbeitung zur übergeordneten Planung und Steuerung der Auftragsabwicklung. Dem Datenmanagement kommt eine entscheidende Bedeutung zu, da Smart Contracts Aufgaben und Transaktionen nur korrekt ausführen können, wenn die im Code hinterlegten Daten aktuell sind. Zudem wird es notwendig, dass zumindest einige Mitarbeiter über Programmierkenntnisse verfügen, um den Code eines Smart Contracts zu verstehen und ggf. notwendige Änderungen vornehmen kann. In die Prozesskostenrechnung wird daher ein Betreuungsaufwand pro Anlage übernommen und ein erhöhter Stundensatz angesetzt, da höhere Qualifizierungsansprüche an die Mitarbeiter gestellt werden.

Auftragsabwicklung	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Konfiguration	80	0,5 h	78 €	3.120 €
Prozessbetreuung	80	1 h	87 €	6.960 €
Prozesskosten Monat				**10.080 €**

Tab. 8: Smart Contract Prozess Auftragsabwicklung

4.3.2 Beschaffung

Die Auswahl der Lieferanten und die Verhandlung von Preisen und Vertragsbedingungen können nicht von Smart Contracts übernommen werden. Bestellungen können als Smart Contracts ausgelöst und über die Blockchain übermittelt werden. Die ausgehandelten Vertragsbedingungen und Konditionen müssen im Code verankert werden. Die Bestellabwicklung kann durch Erfüllen der enthaltenen Bedingungen automatisch durchgeführt werden. Der Prozess in so einem Bestell-Contract kann sich, sehr vereinfacht betrachtet, wie folgt darstellen:

- Bestellanforderung vorhanden → Bestellung auslösen und auf Blockchain an entsprechenden Empfänger übermitteln.
- Bestellung erhalten → Lieferung auslösen.
- Warenausgang → Rechnung auslösen.
- Wareneingang → Rechnung begleichen.

Das Auslösen von Bestellungen kann also vollständig automatisiert werden durch die Integration von Smart Contracts. Auch hier verlagert sich das Aufgabengebiet der Mitarbeiter von der Sachbearbeitung zu übergeordneten Planungs- und Steuerungsaufgaben. Daher wird hier ebenfalls ein Prozessbetreuungsaufwand pro Anlage angesetzt.

Beschaffung	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Prozessbetreuung	80	2 h	87 €	13.920 €
Prozesskosten Monat				**13.920 €**

Tab. 9: Smart Contract Prozess Beschaffung

4.3.3 Kommissionierung

Die Kommissionierung einer Anlage durch den Logistikdienstleister wird durch den Kommissionierungs-Contract des Maschinebauers ausgelöst. Das physische Bereitstellen der Komponenten zum Transport folgt weiterhin dem bisherigen Prozess. Durch die automatisierte Kommissionierung einer Anlage im ERP-System des Logistikdienstleisters kann dennoch eine Prozessverbesserung erreicht werden. Die angesetzte Zeit pro Kommissionierung reduziert sich um 1h. Wareneingangsbuchungen müssen durch das entsprechende Oracle an die Bestell-Contracts übermittelt werden und Erfüllen dadurch deren Bedingung „Wareneingang". Eine konkrete Prozessverkürzung wird dadurch nicht erreicht, daher ändert sich an der Abrechnung nichts. Der durch Smart Contracts generell optimierte Beschaffungsprozess könnte Einfluss auf die benötigte Lagerfläche haben. In diesem Szenario wird vorerst mit den gleichen Werten gerechnet.

Kommissionierung	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Typ A kommissionieren	40	19 h	52 €	39.520 €
Typ B kommissionieren	40	19 h	52 €	39.520 €
WE Buchungen	ca. 7000		1,60 €/Buchung	11.200 €
Belegte qm^2	13.500 m^2		7,20 €/m^2	97.200 €
Prozesskosten Monat				**187.440 €**

Tab. 10: Smart Contract Prozess Kommissionierung

4.3.4 Versand

Der Prozess der Rechnungserstellung und Beauftragung der Spedition wird durch Smart Contracts gesteuert. Wird die Bedingung „Anlage fertig montiert“ erfüllt, wird der Auftrag zum Verpacken ausgelöst und die Spedition zum Transport der Anlage beauftragt. Der Abfahrtsscan erfüllt die Bedingung „Anlage versendet“ und löst die Rechnungserstellung aus. Die Empfangsbestätigung des Kunden und der Zahlungseingang schließen den Smart Contract und damit den gesamten Kundenauftrag ab. Zur Prozessbetreuung werden 0,5h pro Anlage angesetzt.

Versand	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Prozessbetreuung	80	0,5 h	87 €	3.480 €
Prozesskosten Monat				**3.480 €**

Tab. 11: Smart Contract Prozess Versand

4.3.5 Kommunikation

Durch ein dezentral geteiltes Ledger und der damit verbundenen gemeinsamen Datenbasis sind Informationen zu Lieferzeiten, Auftragsstatus, Lagerbeständen, usw. in Echtzeit verfügbar. Die Nachverfolgbarkeit und Eigentumsverhältnisse von Komponenten werden transparent und dauerhaft dokumentiert. Durch die weitestgehend autonome Steuerung der Aufträge und Bestellungen kann der Abstimmungsaufwand deutlich reduziert werden.

Die Smart Contracts lösen sich innerhalb des P2P-Netzwerkes durch Mitteilungen über Änderungen des Status aus. In Abbildung 36 ist das Beziehungsgeflecht abgebildet und die dezentrale Struktur des Netzwerkes wird erkennbar.

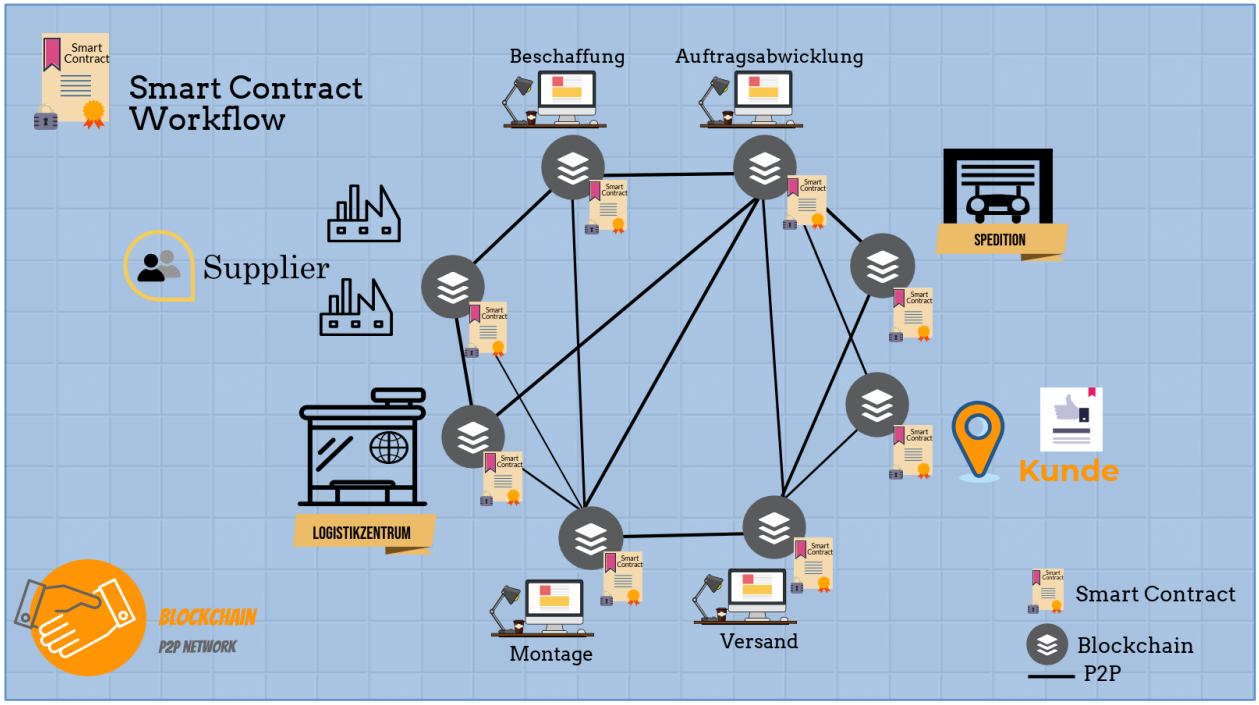

Abb. 36: Blockchain basiertes P2P-Network

Der Abstimmungsaufwand pro Anlage reduziert sich auf 1h.

Abstimmung	Anzahl Vorgänge	Zeit pro Vorgang	Stundensatz	Kosten pro Monat
Prozessbetreuung	80	1 h	87 €	6.960 €
Prozesskosten Monat				**6.960 €**

Tab. 12: Blockchain basierter Abstimmungsprozess

In allen Bereichen werden also Prozesse automatisiert und Aufgabengebiete der Mitarbeiter verschieben sich von der Sachbearbeitung zu übergeordneten Planungs- und Steuerungsaufgaben. Durch die Fähigkeit, Prozesse und Transaktionen selbstständig auszulösen und zu steuern, kann der manuelle Aufwand reduziert werden. Dadurch können auch potenzielle Fehlerquellen und Verzögerungen in der Auftragsabwicklung reduziert werden.

Gesamt	Kosten pro Monat	Anlagen pro Monat	Kosten pro Anlage
Auftragsabwicklung	10.080 €	80	126,00 €
Beschaffung	13.920 €	80	174,00 €
Kommissionierung	187.440 €	80	2.343 €
Versand	3.480 €	80	43,50 €
Abstimmung	6.960 €	80	87,00 €
Prozesskosten Monat	**221.880 €**	**80**	**2.773,50 €**

Tab. 13: Prozesskosten NEU Gesamt

4.4 Schwachstellen & Risiken

Für Unternehmen spielt die Sicherheit ihrer Daten eine wichtige Rolle. Damit Unternehmen bereit sind Informationen über ein Supply Chain Network auszutauschen, muss Vertrauen in das System erreicht werden. Oft sind auch untereinander konkurrierende Unternehmen an einer Supply Chain beteiligt, gerade bei den Supplier. Mögliche Angriffe auf die Datenintegrität oder Manipulationsversuche müssen weitestgehend ausgeschlossen werden. Ausfallsicherheit des Netzwerkes sowie die Transparenz und Rückverfolgbarkeit der Transaktionen sind dabei ein wichtiger Bestandteil, um die notwendige Vertrauensbasis zu schaffen.

4.4.1 P2P-Network

Wie unter 2.3.6 beschrieben sind P2P-Netzwerke dezentral organisierte Systeme, die ohne einen zentralen Server operieren. Jeder Node kann als Server oder Client agieren und ist dabei gleichberechtigt. Dabei besteht das Risiko, dass Nodes unterschiedliche Ziele verfolgen und versuchen könnten, Einfluss auf das Netzwerk zu ihren Gunsten zu nehmen. Fehlerhafte oder Schadsoftware könnte sich sehr schnell im Netzwerk verbreiten. Es muss sichergestellt sein, dass Transaktionen einmalig und vollständig ausgeführt werden.

Durch den Konsensmechanismus des Blockchain Konzeptes können diese Risiken ausgeschlossen werden. Die dezentrale Struktur der Datensicherung sichert die Integrität der in der Blockchain gespeicherten Informationen.

4.4.2 Blockchain

Durch die Verwendung einer privaten Blockchain müssen sich Teilnehmer registrieren und werden durch das Netzwerk autorisiert. Dadurch sind alle Teilnehmer identifizierbar und jede Transaktion kann zum Urheber zurück verfolgt werden. Einmal in einem Block gespeicherte Daten können nicht mehr geändert werden. Durch den fortlaufenden Bezug des Hashwertes eines Blocks zu allen vorangegangen Blöcken würde die Änderung nur eines Bytes den Hashwert des aktuellsten Blocks ändern. Der abweichende Hashwert würde die Blockchain ungültig machen und vom Netzwerk ausschließen. Um unbemerkt Daten einer Blockchain zu manipulieren, müsste ein Angreifer in der Lage sein, die Blockchain auf allen Nodes des Netzwerkes gleichzeitig zu ändern (siehe 2.3.1). Der Konsensmechanismus schafft innerhalb des Netzwerkes Einigkeit und Transparenz über den gültigen Informationsstand (siehe 2.3.5.5). Transaktionen werden durch die Hashfunktion verschlüsselt. Die Hashfunktion transformiert, mittels einer mathematischen Funktion, Informationen in einen Wert der aus Buchstaben und Zahlen in einer bestimmten Länge besteht (siehe 2.3.3). Damit Daten einer Transaktion für Sender und Empfänger lesbar sind, gleichzeitig aber für Unberechtigte verschlüsselt bleiben, wird zusätzlich ein kryptografisches Verfahren verwendet. Dazu wird das Asymmetrische Kryptosystem verwendet, bei dem für Sender und Empfänger jeweils ein eigenes Schlüsselpaar verwendet wird (siehe 2.3.4).

Das Konzept der Blockchain kann also als sicher betrachtet werden.

4.4.3 Smart Contracts

Smart Contracts sind Programmcodes, die auf einer Blockchain laufen und ausführbar sind. Der Code enthält Bedingungen und Regeln, die zwei oder mehr Parteien vereinbart haben. Diese Computerprogramme funktionieren nach dem IF→THEN→ELSE Prinzip (siehe 3.1). Diese Programme sind dabei keineswegs smart, also intelligent, wie der Name vermuten lässt. Smart Contracts sind immer nur so smart wie der enthaltene Code und der wird von Menschen programmiert. Genau hier liegt die große Schwachstelle eines Blockchain basierten Supply Chain Networks. Ein einmal auf der Blockchain installierter Smart Contract kann nicht ohne weiteres Updates erhalten oder revidiert werden. Durch Smart Contracts ausgeführte Transaktionen können nicht einfach geändert oder rückgängig gemacht werden. Fehlerhaft ausgeführte Transaktionen müssen, aufgrund der Unveränderlichkeit der Blockchain, durch nachfolgende Transaktionen korrigiert werden. Daher ist es absolut notwendig, vereinbarte Regeln und Bedingungen korrekt in Code zu übersetzen. Ein fehlerhafter Code könnte dazu genutzt werden, unerwünschte Aktionen auszulösen. Bekanntestes Beispiel hierfür ist der „DAO Hack", bei dem es einem Angreifer gelungen ist, eine Funktion so auszunutzen, dass Ether im Wert von mehreren Millionen Euro auf sein Konto umgeleitet wurde. Nur durch einen sogenannten Hard Fork[14] konnte die Ethereum Blockchain weitergeführt werden. Hacker nutzen Fehler in der Programmierung aus, um ihren Interessen entsprechend Aktionen auszuführen. Der Programmierung und der Überprüfung kommt also eine sehr wesentliche Bedeutung zu. Durch den begrenzten Zugang der privaten Blockchain und das Vergeben von Zugangsberechtigungen sind die Teilnehmer des Netzwerkes bekannt und identifizierbar. Im Grunde ist davon auszugehen, dass in so einem Kooperations-Netzwerk alle Teilnehmer den gleichen Zielen und Interessen folgen. Dennoch können auch unbeabsichtigte Fehler im Code Schaden anrichten. Smart Contracts müssen mit äußerster Sorgfalt programmiert werden. Dazu werden qualifizierte Mitarbeiter benötigt, die in der Lage sind, den Programmcode vollständig zu verstehen und Regeln und Bedingungen korrekt in den Code zu implementieren. Jeder Smart Contract muss bevor er auf der Blockchain implementiert wird, ausführlich in einer sicheren Umgebung nach gängigen Methoden getestet werden. Smart Contracts bleiben dennoch die Schwachstelle eines Blockchain basierten Supply Chain Network.

[14] Ein Hard Fork ist eine Regeländerung der Blockchain. Die nach den alten Regeln validierten Blöcke, werden durch die nach den neuen Regeln produzierten Blöcke als ungültig betrachtet. Im Falle eines Hard Fork müssen alle Nodes, die nach den neuen Regeln arbeiten sollen, ihre Blockchain aktualisieren ("Fork (blockchain)," 2018).

4.4.4 Obstacles

Entscheidend für den Erfolg eines Blockchain basierten Supply Chain Network ist die Kooperationsbereitschaft der beteiligten Unternehmen. Hindernisse bei der Integration einer Blockchain können durch fehlende Bereitschaft der Unternehmen entstehen, wenn Zweifel an der Datensicherheit bestehen. Gerade untereinander konkurrierende Supplier könnten dem System misstrauen und Wettbewerbsnachteile durch Einflussnahme der Konkurrenten befürchten. Zudem müssen die Unternehmen bereit sein, in das Netzwerk zu investieren, sowohl in notwendige Hard- und Software als auch in die Qualifizierung der Mitarbeiter. Es ist also notwendig, die Unternehmen von der Integrität und den potenziellen Vorteilen durch die Prozessoptimierung eines Blockchain basierten Supply Chain Network zu überzeugen.

Unternehmensintern entstehen Hindernisse durch fehlende Bereitschaft der Mitarbeiter, die geänderten Prozesse anzunehmen. Durch den Wegfall von Aufgaben werden viele Mitarbeiter Befürchtungen um ihren Arbeitsplatz haben. Es werden Qualifizierungsmaßnahmen notwendig, um geänderte Aufgabengebiete übernehmen zu können. Durch die frühzeitige Einbeziehung der Belegschaft und des Betriebsrates können Hindernisse überwunden werden. Die Geschäftsführung sollte klar und transparent die Auswirkungen auf Mitarbeiter und Prozessen kommunizieren.

4.5 Wirtschaftlichkeitsbetrachtung

Die notwendigen Investitionen zur Implementierung einer Blockchain und Smart Contracts in das Supply Chain Network werden, dem Szenario folgend, aus Sicht des Maschinenbauers betrachtet. Die Einsparungen der Prozesskosten durch die Integration eines Blockchain basierten Netzwerkes müssen dementsprechend die anstehende Investition rechtfertigen. In der Gesamtbetrachtung (Tab. 14) sind die Prozesskosten des bisherigen und des Blockchain basierten Prozesses gegenübergestellt.

Gesamtbetrachtung	Prozesskosten pro Monat			Prozesskosten pro Anlage		
	Alt	Neu	Diff.	Alt	Neu	Diff.
Auftragsabwicklung	39.640 €	10.080 €	-29.560 €	496 €	126 €	-370 €
Beschaffung	190.152 €	13.920 €	-176.232 €	2.377 €	174 €	-2.203 €
Kommissionierung	191.600 €	187.440 €	-4.160 €	2.395 €	2.343 €	-52 €
Versand	4.140 €	3.480 €	-660 €	52 €	44 €	-8 €
Abstimmung	18.160 €	6.960 €	-11.200 €	227 €	87 €	-140 €
Prozesskosten	**443.692 €**	**221.880 €**	**-221.812 €**	**5.546 €**	**2.774 €**	**-2.773 €**

Tab. 14: Gegenüberstellung der Prozesskosten

Zur Ermittlung der notwendigen Investition wird eine Studie der Beratungsfirma Forrester Consulting herangezogen[15]. Forrester Consulting hat in Kooperation mit IBM eine Studie durchgeführt, um die potenziellen finanziellen Auswirkungen der Integration einer Blockchain Lösung, auf ein Unternehmen zu bewerten. Dazu wurden mehrere Unternehmen befragt, wie sie bei der Integration einer Blockchain Lösung vorgegangen sind. Diese Vorgehensweise wird an das bisher angewendete Szenario angepasst und ergänzt. IBM hat einige Daten zur Verfügung gestellt, bspw.

[15] Die Studie "The Total Economic Impact of IBM Blockchain" ist verfügbar unter: https://public.dhe.ibm.com/common/ssi/ecm/79/en/79017679usen/ibm-blockchain-tei-case-study_final_07-20-2018_79017679USEN.pdf (Odell and Fadzeyeva, 2018).

Lizenzgebühren, Entwicklungskosten durch IBM, etc. Diese Daten werden in die Investitionsrechnung übernommen. Konkrete Finanzdaten zu laufenden Kosten eines Blockchain Netzwerkes, wurden durch die Unternehmen der Studie, nicht zur Verfügung gestellt. Daher hat Forrester Consulting einige Daten auf Grundlage von Best Practise Erfahrung angesetzt. Diese Daten werden ebenfalls an das Szenario angepasst und ergänzt. Der Betrachtungszeitraum beträgt 5 Jahre, da es sich um eine strategische, also langfristig zu betrachtende Entscheidung handelt. In dem Szenario wird davon ausgegangen, die Blockchain nicht vollständig selbst zu entwickeln, sondern das Know How etablierter Unternehmen wie bspw. IBM oder SAP zu nutzen. Es wird ein Projektrisiko von 20% einkalkuliert.

4.5.1 Pilotprojekt Blockchain Prototyp

Das Pilotprojekt dient dazu, das Konzept zu konkretisieren und die Machbarkeit nachzuweisen. Angesetzt für diese Phase werden 6 Monate. Zu Beginn wird ein Design Thinking Workshop durchgeführt, als Teil des Ideen- und Lösungsfindungs-Prozesses. Zwei externe Berater begleiten und moderieren die Erstellung eines Blockchain Prototypen. Aufwände für externe Software Entwicklung fallen bereits an. Für die interne Entwicklung der Software und der IT-Struktur werden 720h angesetzt. Die Entwicklung oder Überarbeitung des Governance Models wird notwendig. Zudem ist es unbedingt erforderlich, mit dem Betriebsrat über mögliche Änderungen von Betriebsvereinbarungen zu verhandeln.

Pilotprojekt Kalkulation	6 Monate
	Initialkosten
Design Thinking Workshop	32.000 €
Consulting: Tagessatz 1.500€	1.500 €
2 Berater 15 Tage/Monat	270.000 €
Software Entwicklung extern	250.000 €
Aufwand IT & Entwicklung	720 h
Stundensatz	91 €
Aufwand IT & Entwicklung	**65.520 €**
Aufwand Governance Konzept & Vertragsverhandlungen	385 h
Stundensatz	101 €
Aufwand Rechtsabteilung	**38.885 €**
Kosten Pilot Projekt	**656.405 €**
Projekt Risiko	20%
Gesamt Kosten Pilotprojekt	**787.686 €**

Tab. 15: Pilotprojekt Kalkulation

4.5.2 Integration und Aufbau des Blockchain Supply Chain Network

Für die Integration der entwickelten Blockchain Lösung wird ein Jahr geplant. Es werden zwei weitere Workshops angesetzt. Die Entwicklungskosten des Systemanbieters werden mit 1.500 T€ angesetzt, zudem werden jährlich Lizenzgebühren fällig. In dieser Phase müssen Mitarbeiter qualifiziert werden, wodurch Kosten für Schulungen und Seminare anfallen. Der interne Aufwand für Entwicklung und IT wird auf 1.440h geschätzt. Für die beschriebenen Prozesse müssen Smart Contracts programmiert werden, wofür 1.600h angesetzt werden. Darin ist bereits das Testen und Validieren der programmierten Smart Contracts enthalten. Für das Finalisieren eines Governance Models und Verhandlungen mit Betriebsräten, Supplier und Kunden werden 1.900h angesetzt. Im ersten Jahr werden Anlaufkosten eingerechnet, um in der Praxis auftretende Probleme zu beheben.

Integration & Aufbau Blockchain SCN	12 Monate
	Initialkosten
Blockchain Entwicklungskosten extern	1.500.000 €
Design Thinking Workshop x2	64.000 €
Blockchain Lizensgebühren	20.000 €
Qualifizierungsmaßnahmen MA	150.000 €
Aufwand IT & Entwicklung	1.440 h
Stundensatz	91 €
Aufwand IT & Entwicklung	**131.040 €**
Aufwand Software Smart Contracts	1.600 h
Stundensatz	91 €
Aufwand IT & Entwicklung	**145.600 €**
Aufwand Governance Konzept & Vertragsverhandlungen	1.900 h
Stundensatz	101 €
Aufwand Rechtsabteilung	**191.900 €**
Anlaufkosten im 1.Jahr	**360.000 €**
Integration & Aufbau Blockchain	**2.562.540 €**
Projekt Risiko	20%
Integration & Aufbau Blockchain	**3.075.048 €**

Tab. 16: Integration & Aufbau Kalkulation

4.5.3 Laufende Kosten Blockchain Supply Chain Network

Jährlich fallen Lizenzgebühren, Wartungsaufwand für das Netzwerk und fortlaufende Entwicklungskosten der Blockchain an. Rechtliche Fragen zu Smart Contracts und anderen Vereinbarungen, das Blockchain Netzwerk betreffend, erfordern eine fortlaufende rechtliche Betreuung. Zudem werden jährliche Kosten für netzwerkbildende bzw. -fördernde Maßnahmen eingeplant. Das können Workshops oder Community Boards sein, zu denen beteiligte Unternehmen eingeladen werden.

Laufende Kosten Blockchain SCN	Jahr
Blockchain Lizenzgebühren	20.000 €
Fortlaufende Blockchain Entwicklungskosten	200.000 €
Wartungsaufwand Blockchain in Stunden	1.152 h
Stundensatz	91 €
Wartungsaufwand Blockchain	**104.832 €**
Aufwand Governance Konzept & Vertragsverhandlungen	1.450 h
Stundensatz	101 €
Aufwand Rechtsabteilung	**146.450 €**
Supply Chain Network Entwicklung (Workshops, Community Boards, etc.)	180.000 €
Laufende Kosten Blockchain	**651.282 €**
Projekt Risiko	20%
Gesamt Kosten Pilot Projekt	**781.538 €**

Tab. 17: Kalkulation Laufende Kosten

4.5.4 Kapitalwert der Investition

Der Kapitalwert bildet den Wert einer Investition nach allen Ein- und Auszahlungen ab. Es wird ein Zinssatz von 7% angesetzt. Die Einzahlungen entsprechen den Prozesskosteneinsparungen. Im ersten operativ aktiven Jahr des Blockchain basierten Netzwerks wird mit Anlaufproblemen gerechnet. In der Integrations-Kalkulation wurden dafür 360 T€ berücksichtigt.

Gesamtdarstellung Blockchain	Initial	Jahr 1	Jahr 2	Jahr 3	Jahr 4	Jahr 5	Total
Einsparung Prozesskosten	**- €**	**2.661.744 €**	**2.661.744 €**	**2.661.744 €**	**2.661.744 €**	**2.661.744 €**	**13.308.720 €**
Kosten Pilot Projekt	-787.686 €	- €	- €	- €	- €	- €	**-787.686 €**
Integration & Aufbau Blockchain	-2.715.048 €	-360.000 €	- €	- €	- €	- €	**-3.075.048 €**
Laufende Kosten Blockchain	- €	-651.282 €	-651.282 €	-651.282 €	-651.282 €	-651.282 €	**-3.256.410 €**
Gesamtkosten inkl. 20% Risk	**-3.502.734 €**	**-1.141.538 €**	**-781.538 €**	**-781.538 €**	**-781.538 €**	**-781.538 €**	**-7.770.426 €**
Ergebnis	**-3.502.734 €**	**1.160.206 €**	**1.880.206 €**	**1.880.206 €**	**1.880.206 €**	**1.880.206 €**	**5.178.294 €**
Kumuliert	-3.502.734 €	-2.342.528 €	-462.323 €	1.417.883 €	3.298.088 €	5.178.294 €	
Abzinsungsfaktor 7%	1,00	1,07	1,14	1,23	1,31	1,40	
Kapitalwert	**-3.502.734 €**	**1.084.304 €**	**1.642.244 €**	**1.534.808 €**	**1.434.400 €**	**1.340.561 €**	**3.533.583 €**

Tab. 18: Kapitalwert Berechnung

Betrachtet auf 5 Jahre ergibt sich auf heute bezogen ein Kapitalwert von 3.534 T€. Also der Wert der sich aus der Differenz der eingesparten Prozesskosten und der Summe der Investitionskosten und den laufenden Kosten ergibt, abgezinst mit 7%. Vereinfacht ausgedrückt wird durch die Investition ein Überschuss von 3.534 T€ erzielt.

Die Amortisationsdauer beträgt 25 Monate.

$$Amortisationsdauer = \frac{\text{Investitionskosten}}{(\text{Kosteneinsparung pro Monat} - \text{Laufende Kosten pro Monat})}$$

$$Amortisationsdauer = \frac{787.686€ + 3.075.048€}{\left(221.812€ - (\frac{781.538€}{12})\right)} = \mathbf{25\ Monate}$$

Der Break-Even-Point wird nach 1.972 Anlagen erreicht. Im Jahr wird mit 960 Anlagen gerechnet (80 Anlagen pro Monat).

$$Break\ even = \frac{\text{Investitionskosten}}{(\text{Kosteneinsparung pro Anlage} - \text{Laufende Kosten pro Anlage})}$$

$$Break\ even = \frac{787.686€ + 3.075.048€}{\left(2.773€ - (\frac{781.538€}{(80 * 12)})\right)} = \mathbf{1.972\ Anlagen}$$

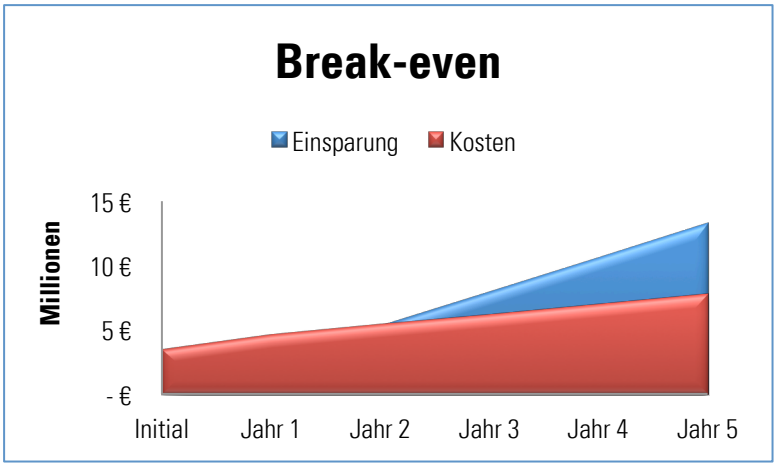

Abb. 37: Break-even Diagramm

Die Investition von 3.863 T€ amortisiert sich also bereits Anfang des dritten Jahres (25. Monat). Der Return on Invest (ROI) auf 5 Jahre betrachtet beträgt 45,5%.

$$ROI = \frac{\text{Kapitalwert}}{Gesamtkosten} * 100 = \frac{3.533.586€}{7.770.426€} * 100 = \mathbf{45,5\%}$$

Die Wirtschaftlichkeit der Investition wird durch die Investitionsrechnung bestätigt. Die Einsparungen durch die Prozessoptimierung wirken sich, auch über den Betrachtungszeitraum von 5 Jahren hinaus positiv aus, wie aus dem im Diagramm zu erkennenden Trend ablesbar ist.

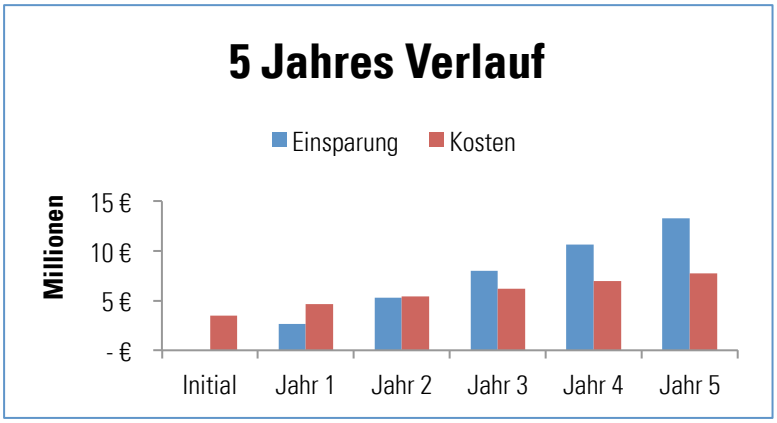

Abb. 38: 5-Jahresverlauf Einsparung – Kosten

Zudem ist zu beachten, dass in die Investitionsrechnung nur die Prozesskosteneinsparungen der betrachteten Prozesse einbezogen wurden, um die Rentabilität zu ermitteln. Es ist durchaus mit zusätzlichen positiven Effekten durch die Integration eines Blockchain basierten Supply Chain Network zu rechnen. Durch die Vernetzung und der in Echtzeit verfügbaren Datenbasis können Lagerbestände reduziert und Transportrouten optimiert werden. Reduzierte Vorrats-Bestände und ein effizienteres Kreditoren- und Debitorenmanagement verringern das im Unternehmen gebundene Kapital. Das wirkt sich positiv auf die Liquidität und den Cash Flow des Unternehmens aus. Dadurch erhöht sich das Rating externer Kapitalgeber und verbessert die Finanzierungsmöglichkeiten des Unternehmens. Die Angebotserstellung und Abstimmungen mit Kunden können effizienter durchgeführt werden wodurch die Cash to cash cycle-time reduziert wird. Durch die Prozessautomatisierung kann es auch zu Personalabbau in einigen Bereichen kommen. Zwar sollte versucht werden alle Mitarbeiter ausreichend zu qualifizieren und in neue Aufgabengebiete zu überführen, dennoch wird ab einem gewissen Grad der Prozessautomatisierung zwangsläufig die Anzahl benötigter Mitarbeiter sinken, was wiederum die Unternehmensrentabilität steigert.

5. Fazit

Nachdem Hype um Bitcoin und Kryptowährungen in 2017 folgte 2018 der Absturz. Bis heute gibt es kaum Möglichkeiten mit Kryptowährung zu bezahlen, sodass ein konkreter Nutzennachweis fehlt. Es werden mehr und mehr Artikel veröffentlicht die bereits das Ende von Bitcoin & Co voraussagen. Dabei wird deutlich, dass Blockchain von vielen immer noch mit Kryptowährung gleichgesetzt wird. Einige Autoren sind der Meinung, dass das Konzept der Blockchain und der Technologie dahinter zu kompliziert sei und sich deshalb nicht durchsetzen wird. Vergleicht man allerdings die Blockchain Technologie mit anderen Softwaresystemen, wie ERP-Systeme oder Bankensysteme, wird schnell klar, dass deutlich kompliziertere Software in der Wirtschaft verwendet wird. Der Gartner Hype Cycle zeigt, dass viele Anwendungen für die Blockchain Technologie im Aufwind sind. Alle großen Firmen, wie IBM, Microsoft, Amazon, SAP etc., arbeiten an Blockchain basierten Lösungen für die Industrie. Dem Hype Cycle folgend steht der Hype um die Technologie noch an, bevor auch hier mit Rückschlägen gerechnet werden muss. Es müssen Lösungen entwickelt und vorgestellt werden, aus denen der wirtschaftliche Nutzen für Unternehmen klar hervorgeht. Letztendlich wird sich eine Technologie nur dann durchsetzen, wenn Wirtschaft und Unternehmen von ihr profitieren. Manager entscheiden rational auf Grundlage eines Kosten-Nutzen Verhältnisses, vereinfacht betrachtet. Aus diesem Grund muss ein exzessiver Hype wie bei den Kryptowährungen, der einen rein spekulativen Hintergrund hatte, nicht befürchtet werden.

5.1 Zusammenfassung

Ziel dieser Arbeit war es Anwendungsmöglichkeiten der Blockchain und Smart Contracts im Supply Chain Management zu identifizieren und dabei auch auf Risiken und Schwachstellen einzugehen. Eine Prozesskotenrechnung und eine Wirtschaftlichkeitsbetrachtung, sollten den Nutzen für das Supply Chain Management belegen. Um Anwendungsfelder und Potenziale erkennen zu können, ist es notwendig die Funktion einer Blockchain zu verstehen. Durch die Geschichte der Blockchain, die eigentlich als Geschichte des Bitcoins viel bekannter ist, konnte eine Abgrenzung der Blockchain von der Funktion „Kryptowährung" vorgenommen werden. Anschließend konnte die Frage nachdem „Warum Blockchain?" beantwortet werden. Die Blockchain kann überall da, wo Transaktionen und die Integrität von Dokumenten nachweisbar sein sollen, als dezentral verteiltes Ledger, eine bisher notwendige dritte Instanz als vertrauenswürdige Clearing Stelle, ersetzen. Im Folgenden wurde die Funktion der Blockchain erklärt. Am Beispiel der Bitcoin Blockchain wurde das Konzept der fortlaufenden Speicherung von Transaktionen in Blöcken und deren Validierung durch den aufeinander aufbauenden Hashwert des Merkle Roots erläutert. Dadurch konnte verdeutlicht werden, dass eine Blockchain im Prinzip fälschungssicher ist. Die verschiedenen Konzepte des Konsensfindungsmechanismus und das kryptografische Verfahren zum Verschlüsseln von Daten wurden erläutert, um die Vertrauenswürdigkeit des Blockchain Konzeptes zu belegen. Anschließend wurde durch ein Anwendungsbeispiel die Funktion von Smart Contracts anschaulich dargestellt. Hier wurden bereits deutlich die Potenziale zur Vereinfachung und Automatisierung von Prozessen sichtbar.

Abschließend wurde ein Szenario entwickelt, welches sich an einer reellen Supply Chain orientierte. Es wurden die Prozesse genauer untersucht, bei denen ein besonders hohes Potenzial zur Prozessoptimierung durch eine Blockchain und Smart Contracts vermutet wurde. Die Auswirkungen durch die Integration einer Blockchain in das Supply Chain Network wurden erläutert und bewertet, ebenso wie die Implementierung von Smart Contracts in die ausgewählten Prozesse. Dabei konnten deutliche Vorteile für alle beteiligten Unternehmen erkennbar werden. Die Prozesskostengegenüberstellung ergab eine Kostenreduzierung von ca. 50% in den betrachteten Prozessen des Maschinenbauers. Als eindeutige Schwachstelle wurden Smart Contracts identifiziert. Fehlerhafter Programmcode kann erheblichen Schaden anrichten. Einmal auf der Blockchain ausgeführte Smart Contracts können nicht ohne weiteres geändert werden. Durch Smart Contracts ausgelöste und durchgeführte Transaktionen können nicht einfach gelöscht oder rückgängig gemacht werden, sondern müssen durch Folgetransaktionen korrigiert werden.

Die Wirtschaftlichkeitsbetrachtung erfasste einen Zeitraum von 5 Jahren. Die notwendige Investition in Höhe von 3,87 Millionen Euro amortisiert sich durch die Prozesskosteneinsparung bereits nach etwas über 2 Jahren (25 Monaten). Der Effekt der Kosteneinsparung wirkt sich über den Betrachtungszeitraum hinaus positiv auf das Betriebsergebnis aus. Der Nachweis der Wirtschaftlichkeit eines Blockchain basierten Supply Chain Network konnte durch den errechneten Kapitalwert von 3,53 Millionen Euro erbracht werden.

5.2 Schlussfolgerungen

Wissenschaft und Wirtschaft sind sich über das Potenzial der Blockchain Kosten zu reduzieren, Prozesse zu optimieren und intermediäre Instanzen zu ersetzen einig. Größtes Hindernis in einem Supply Chain Network wird die notwendige Kooperationsbereitschaft, aller beteiligter Unternehmen sein. Gerade untereinander konkurrierende Supplier könnten Bedenken haben, Daten in einem geteilten Ledger zu teilen. Private Blockchains können dazu beitragen Vertrauen in so ein Netzwerk zu schaffen. Systemanbieter wie IBM, SAP etc., werden durch immer mehr verfügbare Praxisbeispiele den Nutzen der Technologie nachweisen. Vorreiter, also Unternehmen die frühzeitig in eine neue Technologie einsteigen, können Wettbewerbsvorteile erreichen und liefern zugleich Anwendungsbeispiele, denen andere Unternehmen folgen werden. Smart Contracts bieten ebenfalls enormes Potenzial zur Prozessoptimierung und Kostenreduzierung. Allerdings kann nicht erwartet werden, dass jeder Angestellte bspw. im Einkauf oder im Vertrieb in der Lage ist ausgehandelte Konditionen und Bedingungen in Programmcode zu übersetzen. Hier ist es notwendig Lösungen, in Form von DApps zu entwickeln, die es Mitarbeitern ermöglichen Smart Contracts zu erzeugen, ohne das tiefergehende Programmierkenntnisse notwendig sind. Wie beschrieben sind Smart Contracts die größte Schwachstelle des Systems, da fehlerhafter Code ungewünschte Folgen haben kann und zudem einen Angriffspunkt für Manipulationsversuchen bietet.

Ein Blockchain basiertes Netzwerk bietet für Supply Chains enormes Potenzial um Wertschöpfungs- und Lieferketten zu optimieren. Dadurch können Lieferzeiten verkürzt, Transportrouten optimiert und Lagerbestände abgebaut werden. Das Optimierungspotenzial, und damit auch das Potenzial Kosten zu reduzieren, skaliert dabei mit der Größe und dem Grad der Vernetzung eines Supply Chain Network. In unserer global vernetzten Welt konkurrieren heute nicht mehr einzelne Unternehmen miteinander, sondern Supply Chains stehen im Wettbewerb. Daher sind Unternehmen gezwungen kontinuierlich Prozesse zu optimieren. Die Integration der Blockchain Technologie und Smart Contracts, in ein Supply Chain Network, können entscheidende Wettbewerbsvorteile schaffen, zumindest bis konkurrierende Supply Chains nachgezogen haben.

5.3 Resümee

Das Prinzip und die Funktion einer Blockchain und Smart Contracts wurde anhand verfügbarer Literatur, White Paper einiger Blockchain Entwickler und Studienarbeiten von Unternehmen und Beratungsfirmen erläutert. Dabei konnte ein breiter Querschnitt über den Entwicklungsstand, des noch relativ jungen Forschungsgebietes abgebildet werden. Die in der Literatur doch teilweise sehr softwarelastige Entwicklersprache der Autoren, sollte in dieser Arbeit durch eine Praxis orientierte Sprache ersetzt werden, sodass Verantwortliche und Anwender die Technologie verstehen.

Um den Nutzen der Technologie nachzuweisen, wurde ein Szenario entwickelt. Kritisch ist dabei der rein theoretische Ansatz zu betrachten. Zwar hat sich die Arbeit an einem reellen Szenario einer Supply Chain orientiert, der Nachweis zu den Prozessoptimierungen und Kostenreduzierungen bleibt aber reine Theorie. Die Prozesskostenrechnung orientierte sich an realen Werten und die Investitionsaufwände konnten in Teilen von IBM und Forrester Consulting herangezogen werden. Vergleichswerte konnten trotz intensiver Recherche und Anfragen bei Systemanbietern nicht ermittelt werden. Das Potenzial eines Blockchain basierten Supply Chain Network, Prozesse zu optimieren und Kosten zu senken, konnte durch das entwickelte Szenario dennoch deutlich gemacht werden.

6. Literaturverzeichnis

Accenture, General Electric, 2014. Industria Internet Insights Report for 2015 [www]. Abgerufen von: https://www.accenture.com/ch-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Industrial-Internet-Changing-Competitive-Landscape-Industries.pdf (accessed 20.9.18).

Antonopoulos, A.M., 2017. Mastering Bitcoin: programming the open blockchain, Second edition. ed. O'Reilly, Sebastopol, CA.

Bashir, I., 2017. Mastering blockchain: distributed ledgers, decentralization and smart contracts explained. Packt Publishing, Birmingham.

Binärschnittstelle [www], 2018. . Wikipedia. Abgerufen von: https://de.wikipedia.org/w/index.php?title=Bin%C3%A4rschnittstelle&oldid=172936686 (accessed 2.11.18).

Jeff, 2018. Bitcoin Mining Costs by Country | Crescent Electric Supply [www]. Abgerufen von: https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/ (accessed 30.9.18).

BITKOM, VDMA, ZVEI, 2015. Umsetzungsstrategie Industrie 4.0 [www]. Abgerufen von: https://www.bitkom.org/noindex/Publikationen/2015/Leitfaden/Umsetzungsstrategie-Industrie-40/150410-Umsetzungsstrategie-0.pdf (accessed 12.9.18).

BMWi, 2017. Forschungsagenda Industrie 4.0 – Aktualisierung des Forschungsbedarfs (Ergebnisbericht). Berlin, Germany.

Buterin, V., 2017. The Meaning of Decentralization. Vitalik Buterin. Abgerufen von: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274 (accessed 16.9.18).

Cole, A., Gorman, D., 2017. Blockchain Essentials [www]. IBM Devloper Works Courses. Abgerufen von: https://cognitiveclass.ai/courses/blockchain-course/ (accessed 5.10.18).

Czernik, A., 2016. Hashwerte und Hashfunktionen einfach erklärt [www]. Datenschutzbeauftragter. Abgerufen von: https://www.datenschutzbeauftragter-info.de/hashwerte-und-hashfunktionen-einfach-erklaert/ (accessed 8.10.18).

Denial of Service [www], 2018. . Wikipedia. Abgerufen von: https://de.wikipedia.org/w/index.php?title=Denial_of_Service&oldid=181419107 (accessed 31.10.18).

Deutschland, Köhler, H. (Eds.), 2018. Bürgerliches Gesetzbuch: mit Allgemeinem Gleichbehandlungsgesetz, Produkthaftungsgesetz, Unterlassungsklagengesetz, Wohnungseigentumsgesetz, Beurkundungsgesetz und Erbbaurechtsgesetz, 82., überarbeitete Auflage, Stand: 5. Juli 2018, Sonderausgabe. ed, dtv Beck-Texte im dtv. dtv, München.

Dhillon, V., Metcalf, D., Hooper, M., 2017. Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You. Imprint : Apress, Berkeley, CA.

Drescher, D., 2017. Blockchain basics: a non-technical introduction in 25 steps. Apress, Berkeley, California.

Eberspächer, J., Schollmeier, R., 2005. 5. First and Second Generation of Peer-to-Peer Systems, in: Steinmetz, R., Wehrle, K. (Eds.), Peer-to-Peer Systems and Applications. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 35–56. https://doi.org/10.1007/11530657_5

Fork (blockchain) [www], 2018. . Wikipedia. Abgerufen von: https://en.wikipedia.org/w/index.php?title=Fork_(blockchain)&oldid=871146684 (accessed 19.1.19).

Gartner, 2018. Hype Cycle Research Methodology [www]. Abgerufen von: https://www.gartner.com/en/research/methodologies/gartner-hype-cycle (accessed 22.10.18).

GitHub, 2018. Solidity — Solidity 0.4.24 documentation [www]. GitHub. Abgerufen von: https://solidity.readthedocs.io/en/v0.4.24/ (accessed 30.10.18).

Göpfert, I., 2013. Logistik: Führungskonzeption und Management von Supply Chains, 3., aktualisierte und erw. Aufl. ed, Vahlens Handbücher der Wirtschafts- und Sozialwissenschaften. Vahlen, München.

Hahn, C., Wons, A., 2018. Initial Coin Offering (ICO), essentials. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-21787-7

Hardwareabstraktionsschicht [www], 2015. . Wikipedia. Abgerufen von: https://de.wikipedia.org/w/index.php?title=Hardwareabstraktionsschicht&oldid=140885316 (accessed 22.9.18).

Hyperledger, 2018. Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf [www]. hyperledger.org. Abgerufen von: https://www.hyperledger.org/wp-content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf (accessed 30.10.18).

Hyperledger Project, 2017. Hyperledger Project Whitepaper [www]. Abgerufen von: http://www.theblockchain. com/docs/Hyperledger%20Whitepaper.pdf (accessed 30.10.18).

Hyperledger.org, 2018. Hyperledger Blockchain Performance Metrics White Paper [www]. Hyperledger. Abgerufen von: https://www.hyperledger.org/resources/publications/blockchain-performance-metrics (accessed 30.10.18).

Konst, S., 2000. Sichere Log-Dateien auf Grundlage kryptographisch verketteter Einträge. Technische Universität Braunschweig, Braunschweig.

Konstantopoulos, G., 2017. Understanding Blockchain Fundamentals, Part 2: Proof of Work & Proof of Stake. Medium. Abgerufen von: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb (accessed 11.10.18).

Kops, M., 2016. So viel Geld benötigst du für eine Bitcoin-51%-Attacke [www]. BTC-ECHO. Abgerufen von: https://www.btc-echo.de/so-viel-geld-benoetigst-du-fuer-eine-bitcoin-51-attacke/ (accessed 11.10.18).

Malicek, D., 2018. TRON (TRX) [www]. BitContact. Abgerufen von: https://bitcontact.ch/2018/05/23/tron-trx/ (accessed 12.1.19).

Mougayar, W., Buterin, V., 2016. The business blockchain: promise, practice, and application of the next Internet technology. John Wiley & Sons, Inc, Hoboken, New Jersey.

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System [www]. Abgerufen von: https://bitcoin.org/bitcoin.pdf (accessed 22.9.18).

Nier, H., 2018. Die Top 10 der Kryptowährungen [www]. Stat. Infografiken. Abgerufen von: https://de.statista.com/infografik/1939/marktkapitalisierung-von-kryptowaehrungen/ (accessed 1.10.18).

Odell, S., Fadzeyeva, J., 2018. The Total Economic Impact™ Of IBM Blockchain [www]. Forrester Consult. Abgerufen von: https://public.dhe.ibm.com/common/ssi/ecm/79/en/79017679usen/ibm-blockchain-tei-case-study_final_07-20-2018_79017679USEN.pdf (accessed 22.1.19).

Patel, D., Shah, K., Shanbhag, S., Mistry, V., 2018. Towards Legally Enforceable Smart Contracts, in: Chen, S., Wang, H., Zhang, L.-J. (Eds.), Blockchain – ICBC 2018. Springer International Publishing, Cham, pp. 153–165. https://doi.org/10.1007/978-3-319-94478-4_11

Pemberton Levy, H., 2018. The Reality of Blockchain [www]. Gartner.com. Abgerufen von: https://www.gartner.com/smarterwithgartner/the-reality-of-blockchain/ (accessed 21.10.18).

Plattform I4.0, 2013. Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0 [www]. Abgerufen von: http://forschungsunion.de/pdf/industrie_4_0_abschlussbericht.pdf (accessed 17.9.18).

Prinz, W., T.Schulte, A., 2017. Blockchain und Smart Contracts – Technologien, Forschungsfragen und Anwendungen [www]. Fraunhofer Inst. Abgerufen von: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf?_=1516641660 (accessed 16.9.18).

Prof. Dr. Bendel, O., 2018. Definition: Kryptowährung [www]. Gabler Wirtsch. Abgerufen von: https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160/version-277214 (accessed 30.9.18).

PWC, 2016. A look at blockchain technology [www]. BlockchainHub. Abgerufen von: https://blockchainhub.net/blog/infographics/look-blockchain-technology/ (accessed 16.9.18).

Rechtsfähigkeit (Deutschland) [www], 2018. . Wikipedia. Abgerufen von: https://de.wikipedia.org/w/index.php?title=Rechtsf%C3%A4higkeit_(Deutschland)&oldid=181187085 (accessed 29.10.18).

Ries, T., Bersoff, D., Amstrong, C., Adkins, S., Bruening, J., 2017. 2018 Edelman Trust Barometer Global Report [www]. Edelman Trust Barom. Abgerufen von: https://cms.edelman.com/sites/default/files/2018-01/2018%20Edelman%20Trust%20Barometer%20Global%20Report.pdf (accessed 5.10.18).

Rosenberger, P., 2018. Bitcoin und Blockchain: vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. Springer Vieweg, Berlin, Germany.

Sakowski, K., 2018. Grundlagen des Bürgerlichen Rechts, 4., überarbeitete und aktualisierte Auflage. ed. Springer, Berlin.

Schoder, D., Fischbach, K., 2002. Peer-to-Peer. Wirtschaftsinformatik 44, 587–589. https://doi.org/10.1007/BF03250877

Singhal, B., Dhameja, G., Panda, P.S., 2018. Beginning Blockchain: a beginner's guide to building Blockchain solutions. Apress, Berkeley, CA.

smartcontract.com, 2018. Smart Contracts are self-executing contractual states, stored on the blockchain. [www]. Abgerufen von: https://www.smartcontract.com/ (accessed 3.11.18).

Statista.com, 2018a. Google Dossier [www]. Statista. Abgerufen von: https://de.statista.com/statistik/studie/id/6921/dokument/google-statista-dossier/ (accessed 11.9.18).

Statista.com, 2018b. Facebook [www]. Statista. Abgerufen von: https://de.statista.com/statistik/studie/id/3180/dokument/facebook-statista-dossier/ (accessed 11.9.18).

Statista.com, 2018c. Amazon Web Services [www]. Statista. Abgerufen von: https://www.statista.com/study/46913/amazon-web-services/ (accessed 11.9.18).

Statista.com, 2018d. Bitcoin blockchain size 2010-2018 | Statistic [www]. statista.com. Abgerufen von: https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ (accessed 18.10.18).

Swan, M., 2015. Blockchain: blueprint for a new economy, First edition. ed. O'Reilly, Beijing : Sebastopol, CA.

Szabo, N., 1997. The Idea of Smart Contracts [www]. Abgerufen von: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_idea.html (accessed 31.10.18).

Tamayo, D.A., 2017. 1. ibm blockchain explained [www]. Abgerufen von: https://www.slideshare.net/DiegoDiaz49/1-ibm-blockchain-explained/21 (accessed 21.10.18).

Voshmgir, S., Kalinov, V., 2017. Blockchain - A Beginners Guide [www]. blockchainhub.net. Abgerufen von:

https://s3.eu-west-2.amazonaws.com/blockchainhub.media/Blockchain+Technology+Intro.pdf (accessed 24.9.18).

Welzel, C., 2017. Anwendungsszenarien der Blockchain-Technologie in der öffentlichen Verwaltung, in: Kompetenzzentrum Öffentliche IT. Presented at the Fachkongres IT-Planungsrat, Bremen.

Welzel, C., Eckert, K.-P., Kirstein, F., Jacumeit, V., 2017. Mythos Blockchain: Herausforderung für den öffentlichen Sektor, 1st ed. Kompetenzzentrum Öffentliche IT, Fraunhofer Institut für offene Kommunikationssysteme FOKUS, Berlin, Germany.

myetherwallet.com, 2018. What is Gas? · Gas & Transaction Fees | MyEtherWallet Help & Support [www]. What Gas · Gas Trans. Fees MyEtherWallet Help Support. Abgerufen von: https://kb.myetherwallet.com/gas/what-is-gas-ethereum.html (accessed 2.11.18).

Nick Szabo [www], 2018. . Wikipedia. Abgerufen von: https://en.wikipedia.org/w/index.php?title=Nick_Szabo&oldid=859376968 (accessed 22.9.18).

Wood, D.G., 2018. ETHEREUM: A secure decentralised generalised transaction ledger [www]. Abgerufen von: https://ethereum.github.io/yellowpaper/paper.pdf (accessed 25.10.08).

Zeiselmair, A., Bogensperger, A., Hinterstocker, M., 2018. Die Blockchain-Technologie - Chance zur Transformation der Energieversorgung. Forschungsstelle für Energiewirtschaft e.V. (FfE), München.

Zillmann, M., Appel, B., 2016. Supply Chains in der Fertigungsindustrie, in: Supply Chains in der Fertigungsindustrie. Lünendonk GmbH, Mindelheim.

Anhang

Checkliste Transaktionsvalidierung

Checkliste ob die im Blockchain Core Protokoll festgelegten Bedingungen erfüllt werden (Antonopoulos, 2017, p. 220):

- *Syntax und Struktur müssen korrekt sein.*
- *Listen mit Inputs und Outputs dürfen nicht leer sein.*
- *Die Größe der Transaktion in Bytes ist kleiner als MAX_BLOCK_SIZE.*
- *Jeder Output-Wert sowie der Gesamtwert müssen im Bereich der erlaubten Werte liegen (unter 21 Millionen Coins und oberhalb der Dust-Schwelle).*
- *Keiner der Inputs hat hash=0, N=-1 (Coinbase-Transaktionen dürfen nicht weitergeleitet werden).*
- *nLocktime ist gleich INT_MAX, oder nLocktime und nSequence werden entsprechend MedianTimePast erfüllt.*
- *Die Größe der Transaktion in Bytes ist größer oder gleich 100.*
- *Die Anzahl der in der Transaktion enthaltenen Signaturoperationen liegt unter der Grenze für Signaturoperationen.*
- *Das Unlocking-Skript (scriptSig) kann nur Zahlen auf den Stack schieben, und die Locking-Skripte müssen den isStandard-Formen entsprechen. (Nicht dem Standard entsprechende Transaktionen werden also abgelehnt.)*
- *Eine passende Transaktion im Pool oder in einem Block im Hauptzweig muss existieren.*
- *Die Transaktion muss für jeden Input abgelehnt werden, für den der referenzierte Output in einer anderen Transaktion im Pool vorhanden ist.*
- *Für jeden Input wird im Hauptzweig und im Transaktionspool nach der referenzierten Output-Transaktion gesucht. Fehlt die Output-Transaktion für einen Input, handelt es sich um eine verwaiste Transaktion. Sie wird in den Pool verwaister Transaktionen aufgenommen, wenn die passende Transaktion noch nicht im Pool steht.*
- *Ist die referenzierte Output-Transaktion für einen Input ein Coinbase-Output, muss sie mindestens COINBASE_MATURITY (100) Bestätigungen aufweisen.*
- *Der referenzierte Output muss für jeden Input existieren und darf nicht bereits ausgegeben worden sein.*
- *Mit Hilfe der referenzierten Output-Transaktionen, die genutzt werden, um an die Input-Werte zu gelangen, wird geprüft, ob jeder Input-Wert sowie der Gesamtwert innerhalb des erlaubten Wertebereichs liegen (unter 21 Millionen Coins und größer als 0).*
- *Ablehnung, wenn die Summe der Input-Werte kleiner ist als die Summe der Output-Werte.*
- *Ablehnung, wenn die Transaktionsgebühr zu niedrig ist (minRelayTxFee), um in einen Block aufgenommen zu werden.*
- *Die Unlocking-Skripte für jeden Input müssen zu entsprechenden Output-Locking-Skripten passen.*